Security and social implications of radio frequency identification

Thesis · June 2007

CITATIONS
0

READS
1,024

4 authors, including:

Steve F. Russell
Iowa State University
119 PUBLICATIONS **354** CITATIONS

SEE PROFILE

Security and social implications of radio frequency identification

by

Adrienne N. Huffman

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Electrical Engineering

Program of Study Committee:
Steve F. Russell, Major Professor
Thomas Daniels
William Q. Meeker

Iowa State University

Ames, Iowa

2007

DEDICATION

This thesis is dedicated to my family – a group of people who have stood by me and supported me in all my endeavors. Thank you for your help, love, and support!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank everyone who has played a role in helping me with completing my research and helping me review my thesis. Thanks to all my committee members - Dr. Steve Russell, Dr. Thomas Daniels, and Dr. William Meeker – for agreeing to serve on my committee and for all the help and advice you have provided me along the way. Also, thanks to Dr. Mani Mina, Ryan Gerdes, and Pam Myers for your help. A very special thanks to Dr. Srikanta Tirthapura for allowing me to use your RFID equipment and Dr. Langholz of the Iowa State University Small Animal Clinic for allowing me to stop by the clinic for observations. Finally, I would like to thank my mother, Mrs. Cynthia Huffman, for her help with reviewing my thesis. I am extremely grateful for everything each of you has done for me.

ABSTRACT

Radio Frequency Identification (RFID) is a technological advance that has caught the attention of many people. Hailed by some for its ability to overshadow the present day barcode as well as track objects, RFID technology is also ridiculed by many others for reasons that include very little security, *minimal privacy*, and ethical and legal issues. While RFID has the potential to change the way we interact with items on a day-to-day basis, without proper attention, regulation, and security, this technology could prove to be a key that opens Pandora's box.

CHAPTER 1: Introduction

Radio frequency identification (RFID) is a technological advance that has excited many because of the potential it possesses - the potential to do much public good, yet just as much potential to do harm. It has amassed a following because of the convenience, speed, and reliability it is said to hold. Unfortunately, there is concern over the use of RFID because of the minimal privacy and security it holds as well as the social issues it raises.

As we progress further into the 21st century, it is likely that radio frequency identification, a technology that uses radio frequencies to identify an object or set of objects, will continue to grow and expand beyond our wildest dreams. Because of its apparent rooting in supply-chain management, we can at the very least see it utilized by companies for management purposes and replacing the modern day barcode. However, with mention of a desire to create a global network of objects [1] and the application of RFID to humans, one cannot help but to ponder the security of RFID systems and the implications of taking it to the extreme of tagging everything and everyone.

We are not very far away from the reality of a global network of objects as the technology is now inconspicuously present in day-to-day life; most people use some form of it everyday, yet may not be aware of it. However, as RFID has increasingly gained media attention, different groups have asserted concerns over privacy while others have taken their concern over security to the test bench, proving that the technology is not as

secure as it should be for some current and proposed uses, such as for credit card transactions and electronic passports (e-passports).

Despite these concerns, there is an apparent move to press on with further integration of RFID into objects used daily with the intent of providing additional speed, efficiency, reliability, and ultimately security. (Yes, in spite of concerns that RFID is not very secure, one of the ideas behind using an RFID system is to provide some form of extra security.) So, how can successful use of this technology coexist with fears and concerns of privacy invasion and security risks?

This document will address issues dealing with the security and social implications surrounding passive, low frequency RFID systems. While an interest is maintained in all applications of RFID, a major focus is given to an area that has caused a round of controversy and is well suited for the question that has been posed – the implantation of RFID chips into humans. Finally, the concept of fingerprinting RFID signals is presented as a way to add additional security to an RFID system. The viability of this technique is discussed along with experimental results, and the positive and negative consequences of its implementation.

1.1. Historical Overview

Although historically it was not the most pleasant of times, World War II served as a catalyst for growth in radio communications, more specifically, the unprecedented birth of RFID. With Radio Detection and Ranging (RADAR) being introduced by 1935, it was inevitable that the Identification Friend or Foe (IFF) system, a system mentioned in [2] as being a basis for RFID, would soon follow.

Prior to officially being introduced as IFF by the British in the late 1930's, the system was derived from a method in which German airplane pilots would roll their planes when nearing German RADAR systems. This resulted in a change in the signal received on the ground, allowing their countrymen to know whether or not the on-coming aircraft was indeed German. This method has been noted as the first passive RFID system in [2], although the British are officially credited with this in the form of IFF.

By 1945, yet another device penned as an early version of RFID was developed. Inventor, physicist, and musician Leon Theremin invented a device that was to be used as a tool of espionage by the Russian government. The device, historically known as "The Thing", was a passive listening device embedded in a plaque given to U.S. Ambassador Averell Harriman by a group of school children [1,3]. The Thing only operated when a certain frequency was directed toward it.

Development of RFID continued throughout the years as one of the first papers relative to RFID communication, "Communication by Means of Reflected Power" by Harry Stockman, was published in the October 1948 issue of the Proceedings of the IRE. By 1950, major experimentation was underway while the 1960's saw the introduction of electronic article surveillance (EAS) systems in stores for theft protection.

Work on RFID systems continued into the 1970's, which provided a number of RFID influenced projects, including what are considered to be the first of numerous patents granted under the influence of RFID. The first, "Transponder Apparatus & System" filed by Cardullo and Parks in 1970, was granted in 1973 and is credited as an

active RFID system [2,4]. The second, "Remotely Powered Transponder" filed by Works, Murray, Ostroff, and Freedman in 1971, was also granted in 1973 and is credited as keyless entry [2,5]. The 70's is also a time in which new suggestions such as electronic toll collection would arise [6].

By the 1980's, many of the concepts under development in the 70's were actually implemented and by 1991, the first RFID based toll collection system was implemented in Oklahoma. Fast-forward to 2006 and RFID may be found in an array of items used such as automobile remote keyless entry, pet identification systems, library books, patient identification systems, etc. There are also a number of other things under development as we move into the future with this technology. As we push forward, RFID is expected to replace the barcode and enter into the home in ways that can only be imagined.

1.2. How RFID Works

As shown in Figure 1, RFID technology is composed of three main components: the tag (transponder), the reader (transceiver), and the database. Of these, the transponder is likely the most versatile as there are a number of factors that result in it being ideal for a particular application. There are about four distinct components to note within it: its source of power, whether or not it is reprogrammable, its frequency, and its mode and method of sending and receiving data.

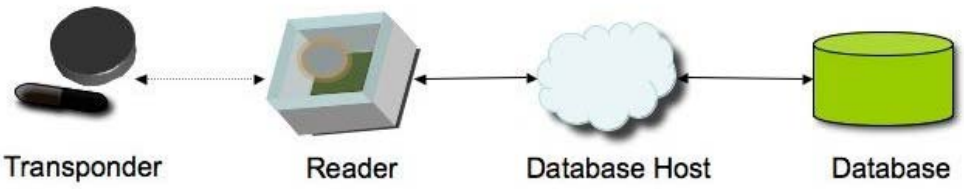


Figure 1 - An RFID System comprised of a transponder, reader, and database.

The method by which the tag receives its power is classified into two categories: active and passive. The active tag source is very straightforward – it uses a battery and can be rendered inoperable if the battery is missing, defective, or depleted. Alternatively, the passive tag receives its power from the RF signal sent from the reader or the magnetic field emitted from the reader's antenna. There are several ways in which this is done: close coupling and inductive coupling use the magnetic field of the reader antenna, while long range devices require electromagnetic (EM) waves. In passive tags, the method for receiving power has a high influence on the range of the device – the ranges that may be achieved include 0 ~ 1cm for close coupling, 0 ~ 1m for inductive coupling, and 1 ~ 3m for long range [7].

Most transponders may be programmed during the manufacturing process. For those that are read-only, a unique serial code or identification number may be programmed so that it cannot be altered later. For those that allow read-write access (programmable), three main types of memory are considered: EEPROM (electrically erasable programmable read only memory), FRAM (ferromagnetic random access memory), and SRAM (static random access memory) [7]. According to [7], the read-write procedure may take place by way of a state-machine or microprocessor.

The frequency at which the RFID system operates is the most important element in terms of communication and range. According to [7], "The operating frequency of an RFID system is the frequency at which the reader transmits." Currently, RFID can operate within four frequency bands, most of which are in the Industrial, Scientific, and

Medical (ISM) Band: the low-frequency band (LF), the high-frequency band (HF), the ultrahigh-frequency band (UHF), and the microwave band [7-11]. When operating within the LF band, the frequency may range from 125 to 134.5kHz. Operation in the HF band is limited to 13.56MHz, while operation in the UHF band may range from 868MHz to 956MHz and also includes the 463MHz band. The Microwave band usually sees operation around 2.45GHz although operation may also occur at 5.8GHz [7,11].

The frequency ranges given are general: only the ranges listed for the LF and HF bands are recognized internationally while ranges within the UHF and Microwave bands are regulated by country. For example, in the UHF band, the United States allows operation in the range of 902MHz to 908MHz. However, it is subject to regulation by the Federal Communications Commission (FCC) CFR 47 Part 15.247 (although sections 245 and 249 should be consulted as well). Europe allows operation within the range of 865MHz to 868MHz, where regulation is subject to the European Telecommunications Standards Institute (ETSI) while Japan and China do not allow any operation within the 868MHz to 956MHz range [10].

Each band has its advantages, disadvantages, and restrictions. It seems as if the very disadvantages for certain bands are the advantages for the other bands. For example, the disadvantage for the LF and HF bands is their lack of range, while range is an advantage for using the UHF and Microwave bands. Alternatively a disadvantage for the UHF and Microwave bands is that certain materials such as liquids and metal may absorb the signal, while the LF and HF bands are minimally affected [10].

The methods in which the data may be sent and received include backscatter, load modulation, sub-harmonics, and the generation of harmonics; while the modes in which the data may be sent and received include full duplex, half-duplex, and sequential [7]. Additionally, there are various types of coding and modulation schemes used in tag-reader communication. According to [7], the baseband coding techniques used in the technology include NRZ, Manchester, Unipolar RZ, Differential Biphase (DBP), Miller, Differential, and Pulse-Pause (PPC). Although there is no particular standard for modulation, the modulation techniques typically used include amplitude shift keying (ASK), phase shift keying (PSK), and frequency shift keying (FSK). [7] mentions that any other modulation techniques used are variations of those given above.

The excitement surrounding RFID and its anticipated replacement of the universal barcode is focused not only on its expected variety of uses, but the cost involved with using them. Many manufacturers will be expected to produce tags for supply chain management and identification for less than the U.S. $0.50 each [12]. While it appears that the cost of using a barcode is limited to the cost of obtaining a unique number and the ink used to print the codes on products, the expected cost of 50 cents per tag does appear to be costly. However, one must also consider the fact that the tag could possibly pay for itself as it is expected to have multiple uses.

1.3 Summary of Remaining Chapters

The remaining chapters are focused on developing issues with and exploring the security and social implications of RFID. Chapter 2 highlights contributions to the discussion of security and social implications of RFID. Applications of RFID will be

reviewed in Chapter 3 while introducing arguments some RFID proponents and opponents make for or against use of the technology. Chapter 4 is focused on the social implications of RFID and also serves as a segue into the discussion on security presented in Chapter 5. Finally, a security alternative is presented in Chapter 6, which outlines the technique of fingerprinting signals.

CHAPTER 2: Contributions to the Study of RFID Security & Social Implications

2.1. Contributions of Others

The topic of radio frequency identification has recently gained momentum as a topic of interest. In particular, interests as they relate to the issues of privacy, security, and the further development of this technology have been addressed via a host of other researchers or individuals who have found a fascination with it. Contributors to the topic as relevant to this thesis range from the United States Government to special interest electronic journals and newsletters.

Despite the range of contributors, this study particularly relies on: information divulged by the organization Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN); information published by the Massachusetts Institute of Technology (MIT) Auto-ID Labs; information collected under the United States Government Department of Homeland Security; information on RFID security provided by authors Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell, and John Kleinschmidt; the RFID research group of Johns Hopkins University; a collection of survey material generated by Christine Perakslis and Robert Wolk of Bridgewater State College; and the research group consisting of John Halamka, Ari Jules, Adam Stubblefield, and Jonathan Westhues. It is of worthy note that Mr. Westhues be mentioned individually as he has made a major contribution in demonstrating how a tag may be cloned and has even provided information regarding how a cloner may be built [13].

Each of the groups named above have made some significant contribution to the study of the security of RFID and the social implications it may have by citing or exploiting the problems the technology has with security or expressing concerns that surround the mainstream implementation of the technology. One group - the research group consisting of Halamka, Jules, Stubblefield, and Westhues - has even suggested an alternative type of tag that may be used for a particular application of RFID [14]. Although many articles and papers relate to the topic of this thesis as suggested by the contributors listed, it is the author's intent to make a contribution that will not only cite the problems of mainstream implementation of the technology, but will also provide an alternative means for securing read-only passive low-frequency identifying tags that utilize a single identifier.

2.2. Contributions of the Author

I have taken a particular interest in the subject matter as a result of exposure to a particular application of RFID that has the potential to serve as a key to opening Pandora's box – the implantation of RFID transponders in humans. Although I maintain a strong opinion regarding the application, I will refrain from interjecting my personal opinion and instead, present the views of others found via a survey distributed to find out information about participants' basic knowledge of RFID and how they regard databases, their privacy and security, and the implantation of tags. While the survey may not be considered scientific, it is supplemented by the findings of Perakslis and Wolk [15].

In addition to the social effects of RFID, I understand there is major concern surrounding the security of RFID systems and will also explore the feasibility of utilizing

the concept of fingerprinting tags as based on a technique for fingerprinting network interface cards (NIC) introduced by the Detecting Intrusion at Layer ONe (DILON) research group of Iowa State University. The practicality of this technique will be addressed by what is thought to be the first step in the process – detection and characterization of an RF signal emitted by passive low frequency tags during tag-to-reader communication. Finally, I will review the pros and cons of fingerprinting RFID transponders.

CHAPTER 3: Applications of RFID

The use of radio frequency identification in society has become more common than one may think. Although reading basic material on the subject matter presents the idea that the technology is limited to supply-chain-management and its anticipated replacement of the bar code along with possible future applications, further reading and an understanding of what RFID entails will show it currently resides in a vast array of applications. A few of the applications that rely on it include (but are not limited to):

- Airline Luggage Identifiers
- Animal Identification
- Automobiles
- Credit Cards
- Electronic Toll Collection
- Electronic Article Surveillance (EAS)
- Home Access
- Library Books
- Medical Alert Devices
- Passports
- Proximity/Access Cards
- Remote Keyless Entry
- Supply-Chain Management

Given these applications are common, it could be assumed that RFID may be easily associated with them since they all can identify a specified object or set of objects by wireless means. However, that is not the case. A survey distributed to 110 individuals ranging in age from 18 to 55 asked the participants several questions regarding their basic knowledge of radio frequency identification. Results showed that while 61.82% were aware of what RFID is, there was a significant variation in listed applications being correctly identified as being or containing RFID. Table 1 displays applications participants were asked to identify along with the resulting percentage of correct responses.

Application	% Correctly Associating Application with RFID
Animal Identification Systems	81.82%
Automobile Remote Keyless Entry	68.18%
Credit Cards	43.64%
Electronic Toll Collection	78.18%
Library Books	65.45%
Luggage Identifiers Printed by Airlines	55.45%
Medical Alert Devices	71.82%
Passports	31.82%
Proximity/Access Card	82.73%

Table 1 - Percentage of survey participants correctly associating given applications with RFID

These results, along with the percentage that were aware of what RFID is, closely compares with those results found in [15], which states that "more than 75% of respondents indicated that they had used or were aware of services using RFID technology, yet respondents did not recognize RFID as the technology utilized in these processes."

3.1 A Controversial Application

There are many proposed applications and enhancements for current applications being considered, which will eventually culminate in the "Internet of Things" – an ad-hoc network established by the arbitrary interaction of RFID tags [1,16]. Applications that are proposed, under development, or being prototyped include:

- Currency
- Home Appliances
- Interactive Grocery Store
- Interactive Smart Homes
- People
- Postage Stamps

As may be seen, the "Internet of Things" is not limited to inanimate objects and animals, it has moved into the realm of use in humans by means of injection.

3.1.1 Why insert? Advocating injection of transponders into people

When we begin to look at social issues such as National security, personal identity, personal security, transactions, emergencies, and tracking, RFID becomes somewhat of a champion for those in distress.

In the wake of the events that transpired in New York City, NY on September 11, 2001, the United States has attempted to maintain a heightened level of security to ensure such an incident never occurs again. Incorporating RFID into identifying objects, documents, and identifiers such as driver's licenses will help the country keep track of those who are deemed "suspicious". By asking citizens to comply with this request, theoretically we will be able to pinpoint troublemakers more quickly and essentially intercept most criminal or terrorist activity. Even if support from citizens is not solicited, RFID devices could be ordered or required to be carried by criminals and those implicated as being involved in terrorist activities – essentially allowing a method of "tracking" incendiaries without imposing on law-abiding citizens.

In terms of personal identity and security, the benefits of using a transponder come in the form of better protection against identity theft. The key to this is the fundamental consolidation of personal information into one device that contains security features, such as challenge-response algorithms, currently applied to computer networks and other wireless entities. Since transponders that can be injected or any other type of transponder proposed to be connected to a human typically are passive and operate at low

frequency, additional security may be found in the short read range of such tags. Also, given the skin will attenuate the signal emitted by the device, the read range will almost certainly be shorter than the read range actually advertised.

In the case of emergencies, RFID may be thought of as a life-saving device. In situations where a person arrives at a hospital, cannot identify him or herself, and has no one present to aid in identifying him or her, a medical attendant can simply query the transponder for the patient's number and identify him or her by matching the number to his or her file which is located in a regional or national database. In addition, the transponder could be configured to operate as a medical alert device.

Finally, for the case of security and access to confidential information, RFID transponders can replace keys – eliminating the need to distribute keys and re-key an office in the event a person's access is revoked. Instead, an access control list (ACL) could be used to control who can and cannot enter an area based on the transponder's identifier. In an office environment, this may fair better than access cards as employees cannot forget to leave the transponder at home. The employer may also save on the cost of replacing damaged badges and even the issuance of cards in general. If employees already have implants, the employer could just as easily obtain the employee's number (with consent) and create an association to it via an association table. The same may be said for the home and automobile.

One thing that may be of particular concern is the use of a single identifying number for multiple applications, which is the equivalent of having one password for all Internet and computer access. However, as mentioned before, the creation of an

association table that creates a new identifier for a particular application may alleviate concerns of the actual number ever being exposed or available for linking to multiple databases.

In summary, injecting transponders into people may help with maintaining National security, may help fight identity theft, may be presumed a life-saving device, allow quick access and transactions, and can provide better access to private and/or confidential information and/or locations.

3.1.2 Why not insert? Criticizing the injection of transponders into people

The same reasons for inserting a tag may also be used in an argument against inserting tags.

National Security is a major government concern in the post 9/11 era. However, the idea that American citizens will willingly submit to having a tag inserted into them to help maintain national security is rather optimistic. Results from the survey distributed on behalf of this thesis indicate that in terms of being most important, national security ranked third when compared to personal security, privacy, and religious beliefs. Additionally, outrage may ensue if criminals are forced to carry RFID devices; human rights may be viewed as violated and question of what will prohibit the government from enforcing this policy on law-abiding citizens will arise. This results in the concern of abuse of power. [15] cites the 1997 U.S. Privacy Protection Study Commission as suggesting, "the real danger is the gradual erosion of individual liberties, through the automation, integration, and interconnection of many small, separate record keeping

systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."

In the case of using RFID for personal identity and security, placing or associating multiple applications to a single number or identifier will place an individual at greater risk for sensitive information to be compromised and stolen. Also, if everything is linked to or stored in a single database, a breach of that database would result in the compromise of all general information rather than application specific information. Even though the short read range of a transponder and use of cryptographic functions add additional security, there are several additional things to consider:

Limitation of Security Features. The type of security features such as cryptographic functions and challenge-response algorithms that may be used (as well as the complexity of such functions) will be limited by the size of the transponder and how much memory it contains. This is likely to have a direct correlation to the cost of the chip.

Rogue Reading. Directional high-gain antennas may be used to achieve a larger read range from the signal. Although the type of tag and reader used is not identified, in 2005 a read range of 69ft was achieved in a competition geared toward exploiting or extending the read range of a tag [17]. Even if a specialized antenna does not extend the read range it would still only take a stranger bumping into you or even just passing by to have a transponder queried by a reader the person may have hidden under clothing or as an accessory.

In terms of emergencies, while an inserted RFID transponder may be deemed a life-saving device, heavy consideration should be given to events in which there is a loss of power, the database can't be accessed due to low bandwidth, or the host for the database becomes inoperable or is compromised. These are major problems and concerns that already plague systems that have become digitized (not just in the medical realm). While the likelihood such events would take place frequently is low, they are still threats that could undermine the advantage RFID is suggested to have.

Finally, for the case of security and access to confidential information, several groups have indicated that use of RFID alone for authentication purposes is not reliable. [18] even mentions that alternative solutions for identification should be explored. The point regarding unreliable authentication also lends itself to the issue of using RFID for access control and transactions. Within this category are also issues concerning other forms of manipulation such as jamming and hacking as well as physical damage and loss of power.

Overall, RFID may be considered a cure-all for sensitive applications when it is only a quick fix. As technology advances, so does the knowledge and capabilities of people looking to undermine specific arenas. The introduction of RFID in the manner of a person playing host for a transponder will only make it easier for criminals and the like to obtain the objects of their desire.

3.2 RFID Warfare

As may be seen by the arguments that have been presented, two major concerns with the implementation of any RFID system are privacy and security. Because of this,

no matter what argument is pursued, a great deal of emphasis is placed on securing a system as well and as cost efficiently as possible. Despite this common goal, the arguments presented demonstrate that for each reason for or against applying RFID to humans (or any other application) the opposing side can present feasible reasoning as to why the view presented by the opposition will not work or can be altered in favor of the opposition. This ultimately results in a cycle of RFID warfare.

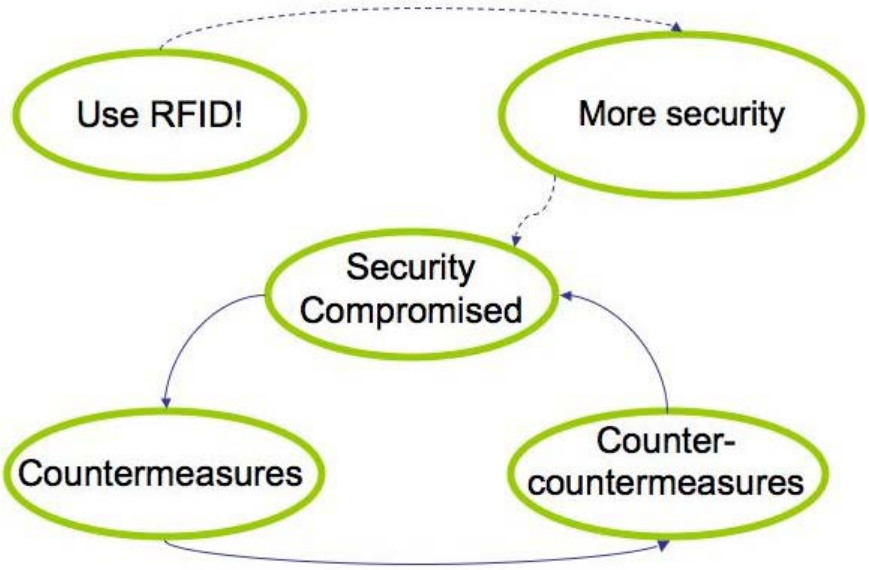


Figure 2 - RFID Warfare Cycle presented from a security standpoint.

This cycle of warfare, which is illustrated in Figure 2, is an observation we have made in reviewing the arguments presented by RFID proponents and opponents. An idea or application is presented that offers added privacy and security along with the other benefits of using it. In a matter of time, the security is compromised and measures are eventually established to counter the compromise. Counter-counter measures soon follow, resulting in yet another security compromise and ultimately, a repetitive cycle

that is only broken by the introduction of another form of technology. The cycle is then reinstated with the new technology.

The RFID Warfare Cycle may be complimented by the technology adoption lifecycle represented by Rogers' Innovation Adoption Curve. As depicted by [19] and represented in Figure 3, the life of technology begins with Innovators, those who want to adopt newer technology for the sake of it. Followed by the Innovators are the Early Adapters, people who want to adopt a new technology because they can see a beneficial application for it. Not represented on the curve is the Chasm, a critical stage in the development of technology that serves as a phase between the Early Adapters and initial mainstream implementation of the technology, the stage applicable to the Early Majority. The Early Majority, those who are ready to find the advantages of the tested technology, leads those considered to be the Late Majority – Traditionalists who are reluctant to give into a technology, but eventually do so. The final group consists of Traditionalists who are considered to be Laggards – those not wanting to accept the technology and question its worth.

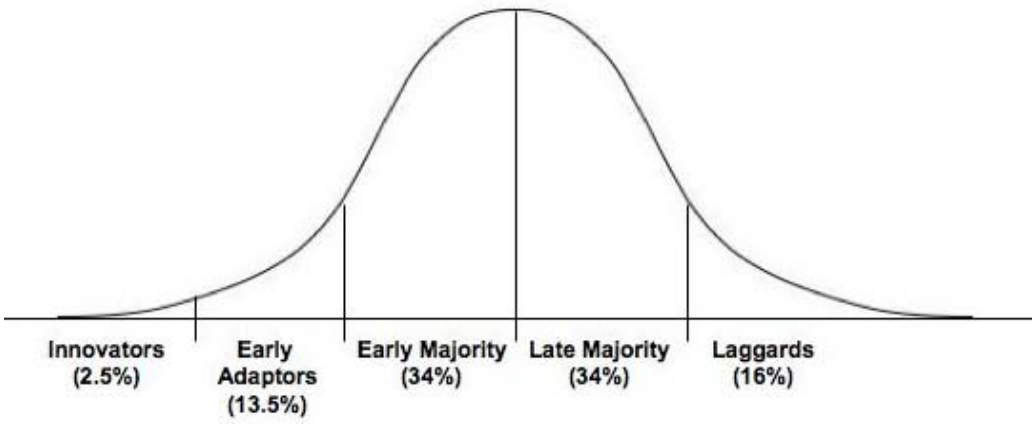


Figure 3 - Rogers' Innovation Adoption Curve.

When viewing the RFID Warfare Cycle and Rogers' Innovation Adoption Curve as a pair, the RFID Warfare Cycle may be viewed as an ongoing battle between Traditionalists and those choosing to adopt the technology. Since it is not guaranteed that a technology will pass the Chasm stage, either cycle can cease before reaching mainstream implementation.

CHAPTER 4: Social Implications of RFID

RFID technology has established a latent presence in society, as may be inferred by the list of some current applications given in Chapter 3. However, given the RFID warfare cycle, the question of its worth in certain applications arises. Essentially, the core issues surrounding RFID that continually arise include: privacy; inconveniences; health risks and concerns; and ethical and legal issues.

4.1 Privacy

The main advantages of using RFID – speed, efficiency, and reliability – are also poised to become the crux for disadvantages. By eliminating the need to have physical contact for device communication and replacing it with proximity communication [20], what was thought to be private communication has, in some ways, become open communication. This may be understood through the following example. If you are in a room of people and only want to communicate information with one person, you may find that person and look them face-to-face while speaking to him or her. However, an open communication system may be synonymous with being in that same room of people and yelling across the room to the individual you wish to communicate information with, all while in hopes that others in the room will continue with their personal conversations and ignore your conversation.

This is the problem that is presented with RFID – essentially broadcasting information across a room with hopes that no others are listening. While transponders are limited in range, the fact that information can be relayed in open air versus physical contact raises alarms for those interested in maintaining privacy. Although the survey

distributed by the author indicates that 50% of participants view privacy as extremely important, Perakslis and Wolk indicate, "…privacy [is a] chief concern in all nations for the usages of RFID, Biometrics, and the fused usages of Biometrics with RFID (including implantable chips)."

Before moving any further into this discussion, it is important to define the term privacy. [21] provides a good definition of both privacy and security that will be used in the remainder of this document. Privacy is defined as, "when and with whom you share your personal information," and security is defined as, "how well your information is protected from unauthorized access, alteration, or destruction."

Referring back to the transponder, the authors of [20] performed experiments with RFID-enabled credit cards that demonstrated most cards reveal very sensitive information, including: the cardholder's name, the complete credit card number, the credit card expiration date, the credit card type, and relevant information about the software version and supported protocols. They were also successful in performing attacks that included skimming, eavesdropping, and replay attacks.

In addition to privacy issues raised by RFID-enabled credit cards, concerns have been raised regarding the use of RFID in passports. [22] suggests that in adopting e-passports, the United States is following guidelines set forth by the United Nation's International Civil Aviation Organization (ICAO), which maintains that RFID-enabled passports should contain the passport holder's name, date of birth, and passport number in the memory. This is verified in [23], which shows that for the United States, the RFID chip will also contain the nationality, sex, place of birth, a digital photograph, passport

issue and expiration date, and the type of passport issued. Although a Faraday cage housing is used to physically protect the data when the passport is not in operation and a cryptographic function for passive authentication and an optional cryptographic function for active authentication is used when it is in operation, the major risk of privacy invasion still occurs when the passport is in use. When engaged, [22] reports that among other things, there is a risk of eavesdropping and data leakage, which may lead to identity theft, tracking, and hotlisting despite the implementation of a cryptographic function. Additionally, it is noted in [24] that the United States Department of Homeland Security (DHS) plans to keep data gathered from passport readers for 75 years. If information from all passport readers is piped into a single database, another problem will ensue depending on the sensitivity of the information being stored. The issue of using databases in an RFID system is further discussed in Chapter 5.

To understand the privacy implications of using a centralized mainstream RFID system, it is necessary to take a look at those implications that occur with currently implemented RFID systems. Viviane Reding, Commissioner of the European Information Society & Media, mentioned in [25] that 1 billion RFID-enabled devices exist worldwide and that this number is projected to grow 500 times (to 500 billion) within the next 10 years. At this rate of growth, it is necessary to address the privacy issues presented by commonly used systems. Accordingly, DHS's Data Privacy & Integrity Committee presents the question, "… do privacy and security concerns outweigh the incremental benefits gained by using an RFID-enabled system over a system poising fewer privacy and security risks? [18]"

4.2 Inconveniences

In understanding the inconveniences that may occur in an RFID system, one may take a look at those things that are likely to inhibit the operation of a system.

Transponder Placement. In the case of human insertion, a person will need to see a specialist to have the chip inserted [26]. Because human skin is not as pliable as the skin of animals such as cats or dogs, insertion may result in pain and/or damage. Also, there exists the likelihood that multiple attempts to insert the transponder correctly will be needed. In the case of other applications where a high accuracy rate coupled with speed is desired, such as warehouses and e-toll collection, the placement of the tag is important dependent on the type of antenna and labeling used.

Transponder Aging. Although passive tags do not carry a power supply and are advertised as surviving the life of the host, realistically, the components used for creating the transponder will experience aging. At some point in time, this may cause degradation in the tag's acceptance rate. In the event that a high acceptance rate is desired and replacement becomes necessary, the process of removal from a human will likely be painful and tedious as the tag can migrate unless a protein coating is used or the tag capsule is porous, allowing for skin, etc. to grow into and around it. In the case of the later, removal may be extremely painful if a local anesthetic is not used [26].

Transponder, Reader Operation and Reliability. There are many circumstances in which the tag may not work, the reader may not work, or there is a complete breakdown in communication. [14] reports that, due to manufacturing, tags may

experience a 5% failure rate. Other sources of failure include whether or not the system is correctly installed or implemented; malicious activity occurring in the proximity of the system; situational events such as power outages, blackouts, brownouts, isolated loss of power to the reader (accidental and otherwise); reader settings not appropriate for communication with a particular tag; and, unknown and/or unintended damage (physical and otherwise) to either apparatus. In fact, Perakslis and Wolk have found another study to confirm that 66% of consumers find it worse to have access to a system denied to him or her due to glitches than to have a system that does not rely on proving his or her identity.

Compromise Recovery. In the event a system is compromised, "…the thorny question arises of how to re-establish access rights for compromised devices. [14]" For example, a person is carrying a transponder embedded under his or her skin, and someone clones that person's information. The clone successfully grants access to the targeted system, resulting in a system compromise. In attempting to re-establish access rights, it would not be logical to reuse the identifier that resulted in the compromise and the person who was originally granted access may not want to undergo transponder replacement. This is likely why it is not recommended that RFID be used alone for authentication and security purposes [14,18]. Special consideration must also be taken if biometrics is also used as a supplement for flaws in the system – this will further complicate how the problem may be resolved.

Cost of Support. An argument for RFID is the expected minimal cost for transponders. Unfortunately, this low-cost is not extended to readers and databases –

the other key components of an RFID system. Although the cost of upkeep will vary by application and implementation, it should be safe to say that the reader and database will prove to be the costliest, especially when considering the use of passive tags. Just as a transponder ages, so will a reader. It will also be necessary to pay for power to the reader and database host. Database upkeep will be contingent on the upkeep of the host for the database, be it a desktop computer, the reader itself, a server, or even a mobile telephone or personal digital assistant (PDA). These circumstances should be taken into consideration when comparing an RFID-enabled system to its standard counterpart (e.g. a lock & key system).

4.3 Health Risks & Concerns

In the age of the mobile telephone, a particular awareness has been raised about the effects of radiation and the effects on health that may result from exposure to radiation. As a result, radio frequency identification, particularly the use of it in humans, may come under the same scrutiny as cellular telephones have gone under because of its intended daily use and possibly being embedded in the body.

In the survey distributed to find out more about how participants feel about RFID, 75.45% of respondents suggested they would not opt to have a transponder – one that would link them to their medical records, allow them to make financial transactions without pulling out a card or checkbook, and allow them access to their car, home, or any other location without the use of a key – injected into their hand. Of those that do not favor insertion, 15.66% cited medical concerns as prohibiting them from having the chips injected. Although we have moved a step closer to using injected transponders in a

centralized identification system through the introduction of VeriMed, an RFID system for at-risk medical patients that uses the VeriChip transponder [27], there are still concerns relevant to how such devices may affect health if widespread implementation occurs, including: possibility of an allergic reaction, the body rejecting the tag, and whether or not the radiation involved with tag-transponder communication is strong enough to have a negative side effect if continuously used over an extended period of time.

These concerns are also addressed in an October 2004 letter CASPIAN found addressed from the FDA to the then Vice President of Finance and Chief Financial Office for Digital Angel Corporation:

> *"The potential risks to health associated with the device are: adverse tissue reaction; migration of implanted transponder; compromised information security; failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick. The special controls document aids in mitigating the risks by identifying performance and safety testing, and appropriate labeling. Thus, in addition to the general controls of the act, an Implantable Radiofrequency Transponder System for Patient Identification and Health Information is subject to the following special control: Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information."* [28, 29]

Despite this warning, the amount of radiation a person is exposed to when participating in a RFID system is thought to be considerably low. However, it is suggested that future studies on the health concerns and issues incorporate what kind of long-term effects may result from continuous exposure to low amounts of radiation.

4.4 Ethical & Legal Issues

Other issues surrounding the use of a centralized RFID system include those relevant to ethics and law. Issues congruent to this matter include (but are not limited to) exclusion based on religious preferences, public knowledge of the technology, and identity theft among other crimes.

Unlike newer forms of technology, RFID has brought upon a general concern by some as a result of religious beliefs. Christians have been cited as being one of the major opponents to the use of RFID because of a passage from the book of Revelations in the Christian Bible:

> *"He also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead, so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name. This calls for wisdom. If anyone has insight, let him calculate the number of the beast, for it is man's number. His number is 666."* [30]

If the required use of this electronic ID were to prevail, the posed concern may easily turn into fear of exclusion based on such preferences.

In the distributed survey, 18.07% of participants cited religious beliefs as the prohibitor for inserting or injecting a chip into themselves. Although participants were not asked to identify their religious preference, according to [31] approximately 32% of the world population and 75% of U.S. and Canadian adults have been identified as Christian. Assuming all individuals included in the statistics consciously deny the use of RFID, an enormous portion of the world population would be excluded! If RFID were to become a standard across the globe, the question of what could be done by this group, and other groups, to circumvent exclusion arises.

It may be because of this, among many other reasons, laws in the United States have emerged that are relevant to the use of RFID. States that have either introduced or passed legislation concerning the technology include:

- California
- Maryland
- Massachusetts
- Missouri
- Nevada
- New Hampshire
- New Mexico
- Rhode Island
- South Dakota
- Utah
- Tennessee
- Texas
- Wisconsin

In addition to the laws offered by these states, there are national laws that have been drafted or are in place that either directly or indirectly reference the technology. On October 25, 2005, the U.S. Department of State implemented a rule that required all U.S. passports to begin transition into an electronic passport containing RFID [23].

While it does not explicitly mention RFID as the technology of choice, the REAL ID Act of 2005 alludes to the implementation of RFID in state issued drivers licenses (among other forms of electronic identifiers such as magnetic strips) [32]. Originally, the Act was to affect all licenses issued before (and after) May 11, 2008. However, due to state opposition, the new deadline has been delayed until 2009 [33].

Another point of legislation is the RFID Right to Know Act of 2003, which was drafted by CASPIAN. This would, if formally introduced and passed, essentially require those utilizing RFID to let consumers know about the use or implementation of the technology up-front, limit the use of RFID enabled devices, and assert public education

of the technology. Although it apparently has not been ratified, some of the issues it brings forth have been adopted in the proposed legislation for the previously listed states.

One of the most important provisions of the drafted Act is public education. In the survey that was administered for support of this thesis, participants were asked to identify nine items as either being or containing RFID in addition to being asked whether or not they were aware of legislation or proposed legislation regarding RFID. While results to the question regarding identification may be found in Table I of Chapter 4, there is a significant variation in the items that were correctly identified. The results also revealed that 90.91% were unaware of current or proposed legislation concerning radio frequency identification. To further solidify the importance of public education, [18] emphasizes educating the mass about RFID technology as a main point in considering the use of RFID for human identity verification.

The question of ethics mainly lies in how an RFID system is implemented, how the system is used, and how information is retrieved from the system upon implementation. It appears that most companies and other groups that have begun distribution of an RFID system have attempted to do so quietly and without explaining what it is and the consequences that may occur from using them. One such situation involves a group of children in a Northern California school district who were forced to wear RFID enabled badges without parental knowledge or consent [34,35]. Once parents were alerted to this, the program was dissolved because of public outrage. Even if wearing the badge was presented as optional, the benefits a student could receive from wearing them could have left the perception that they were required as suggested by [36].

Other situations involve trial runs of RFID enabled consumer products. [1,37] mentions that Proctor & Gamble ran a trial in association with a Broken Arrow, OK Wal-Mart store, in which a particular product line contained a hidden RFID transponder. This allowed Proctor & Gamble researchers 750 miles away to know when the product was picked up, when inventory was low, and even see an image of customers who were exploring the product. Unfortunately, customers were not informed of this trial and after [36] appeared, denials of performing the trial arose until undeniable evidence proved otherwise [1]. In the case where implanted tags are perceived as a voluntary action

Cause for concern not only lies with companies and other RFID interest groups, it lies with the government and individuals. Many have a concern about the possible abuse of government power that may come with the introduction of any kind of electronic identification system - the main concern dealing with possible loss of privacy and eventual tracking. Results from the survey distributed for this thesis show that 84.55% of survey participants would be concerned if the government were to mandate implanted RFID tags. Of those who would be concerned, 68.82% noted they would attempt to lobby or campaign against the mandate. As an alternative, if the option of carrying rather than implanting the tag were presented, 60.91% noted they would be concerned, and of those, 70.15% would attempt to lobby or campaign against the mandate.

As mentioned in Chapter 3, one of the main reasons for introducing a centralized mainstream RFID system is to help consumers better deal with identity theft. Unfortunately, the security threats presented in Chapter 5 prevent this ideology from being feasible. As an example, the sensitive information contained on an e-passport

could be used to create a virtual image of the victim. Therefore, the introduction of new and tougher legislation only solves one part of the equation; the other half deals with the question of how to enforce those laws and ensure compromising activity is low. Unfortunately, this will be tough to deal with, as compromising activity may be less likely to be detected given that communication of data is airborne.

CHAPTER 5: Security of RFID

A quote made by Ari Juels of RSA Labs in [38] reads, "The world of RFID is like the Internet in its early stages… Nobody thought about building security features into the Internet in advance, and now we're paying for it in viruses and other attacks. We're likely to see the same thing with RFIDs." This viewpoint summarizes one of the main problems with RFID – no development of security features in the early stages. So, in regards to the issue of security, the question therefore becomes, not if, but when will this technology be compromised.

5.1 Constraints

5.1.1 Transponder Size

Transponders come in a variety of shapes and sizes – some being advertised as small as a spec of powder at 50.8μm by 50.8μm [39]. Those transponders referenced in this document are thought to be similar in size to those experimentally injected in humans in addition to transponders that we measure to be roughly the size of an aspirin. These small sizes tend to prohibit a tag from containing any security measures since the memory is constrained by physical limitations. This is something that may not be an issue in the future as new methods of decreasing the physical size of storage (increasing the amount of memory) are introduced.

5.1.2 RFID System Range

Naturally, the range of an RFID system plays a large role in the security of that system. According to [40], the constraints affecting the achievable range of an RFID system are the radiated field strength and electromagnetics.

[40] summarizes radiated field strength as, "…directly limited by regulations, and through regulatory and hardware bandwidth constraints, influenced indirectly by communications." Regulations for RFID devices are typically limited to government regulation by frequency range and standards that may exist for different applications.

As mentioned in the introduction and Chapter 3, tags under consideration are passive and low frequency in nature. In the United States, if an RFID system radiates, it is subject to regulation by the FCC. However, if the system is reliant on mutual inductance, it will not be subject to government regulation since it is not a radiator; regulation would only ensue in the event a system causes some interference. For other countries, the issue of interference may soon be addressed by the introduction of policy such as the European Licensing Act for Inductive Radio Systems, which defines a 49kHz zone between 70kHz and 119kHz that may not be used by RFID equipment [41].

Other standards do exist, but as mentioned, vary by application. For example, EPCglobal is found to hold a standard for electronic product codes (EPC), while the International Organization for Standardization (ISO) holds multiple standards, including one for proximity coupling contactless smartcards (ISO 14443) and animal tracking and identification (ISO 11784/11785). Unfortunately, multiple standards may exist for a particular application, which leads to the problem of interoperability and numbering.

Constraints on the hardware have just as large an effect on the amount of energy radiated as the aforementioned constraints. The configuration of the tag circuit load also has an effect on the range because of the varying number of components needed to suit a particular application. For instance, a tag may incorporate functions such as signal processing, memory storage, cryptography, and anti-collision techniques while another tag may incorporate only signal processing and memory storage. In either case, power is needed to drive the components needed to complete the functions! If power cannot be provided at the desired distance, then either the tag has to be moved closer to the reader or the power or antenna gain will need to be increased in order to facilitate the functions provided in the tag [7].

The main determinant of the electromagnetics constraint is whether or not the transponder lays in the near or far field of the reader. The near field is described as the field in which the magnetic field resides. This area starts at the antenna and extends to approximately $\lambda/2\pi$, where λ represents the wavelength [7]. Frequencies that operate within the near field are generally noted as being less than 30MHz. While the tag uses coupling (capacitive or inductive) to receive power, it is standard practice to use a load modulation technique when using a LF or HF passive tag within this field. Load modulation occurs when amplitude modulation is simulated in the transponder by the switching on and off of a load resistor near the antenna. With data controlling the timing of the switching, the information is transmitted from the transponder to the reader where demodulation occurs by way of a rectifier [40].

Once the $\lambda/2\pi$ mark is passed, the electromagnetic field separates from the antenna and begins propagating as an electromagnetic wave [7]. This area is known as the far field and it is within this field that the use of EM waves (long range) to power tags occurs. Standard practice demonstrates that the backscatter modulation technique is used and that frequencies operating in this field are typically greater than 30MHz. However, as previously mentioned, this study primarily focuses on passive low-frequency transponders. Therefore, transponders discussed in this study operate in the near field, using load modulation and inductive coupling.

5.1.3 Antenna Selection & Orientation

There are a number of types of antennas used within the tag and reader including: the single dipole and dual dipole antennas for tags, and linear and circular loop antennas for readers. Although other types exist, those mentioned above will serve as the basis for discussion.

The type of antenna selected and the orientation of the antenna can have an interesting effect on the amount of energy radiated. The single dipole and other similar linear antennas can provide modest directionality of coverage, while the dual dipole and circular loop antennas provide more of an omni-directional coverage. An example of the effect orientation has may be found in the illustrations given in [42], which show that a single dipole antenna chosen for a tag and placed parallel to a linear antenna chosen for the reader will receive good coverage, while the same tag's antenna placed perpendicular to the reader antenna will not – a concept defined as polarization mismatch. However,

using the same tag with a circular loop antenna chosen for the reader will provide good coverage in either orientation.

5.2 Threats to RFID Security

So far, the size and range of a transponder have been identified as points of threats to the security of an RFID system. However, there are numerous other threats, some which have yet to be identified. With the help of information provided in [43] and additional observations, we have categorized a list of known threats to an RFID system, which is shown in Table 3 by the point at which they occur.

Point	Threat
Tag	• Blocking • Physical Damage • Range • Size
Airlink	• Denial of Service (DoS) • Replay • Spoofing
Reader	• Impersonation (Rogue Reader) • Malicious Code • Physical Damage
Database	• Hacking • Human/Software Error • Malicious Code • Physical Damage • Theft

Table 2 - Security Threats of an RFID System by Point of Threat

5.2.1 Tag Threats

As mentioned in [43], one of the attacks that can occur against an RFID system is actually blocking a tag from a reader. It is widely known that by placing a strip of aluminum foil – or a thin strip of foil enveloping a thin layer of salt-water solution – over

a tag, the tag can be blocked from sending or receiving a signal. This type of attack would more specifically affect store merchandise as it may now become more susceptible to petty theft.

Additionally, the transponder is also susceptible to physical damage. A tag may be disabled or destroyed in a microwave oven in as little as two to three seconds [1]. Tampering with or destroying the circuit and/or antenna may also destroy it. In all cases, damage to the tag will result in it no longer being operable and thus undetectable. Again, such actions are particularly relevant in the case of store merchandise containing a transponder.

5.2.2 Airlink Threats

Between the transponder and the reader lies the airlink. This area is probably the second most vulnerable spot in an RFID system, as the information flow cannot be physically protected. Threats to the security of an RFID system at this point fall as prey to attacks that occur to many other wireless systems and computer networks. One such attack is the Denial-of-Service (DoS) attack.

A DoS attack may occur when too many tags are placed near a reader, especially when the reader does not employ anti-collision measures. So, from the perspective of a reader, simply placing two or more transponders in the reader's field will jam the airlink. Similar attacks may occur by using an unrelated device such as a frequency generator to create enough signal noise to cloud or cancel the desired signal. Other DoS attacks may occur in the form of physically altering the surrounding environment to increase the likelihood of multipath and fading, which could essentially cancel the desired signal

altogether. Physical alteration of the system may also lead to DoS in cases where power to and from the reader is cut or eliminated.

Spoofing is also a likely threat. Instead of waiting to record or clone a tag, a determined person may attempt a brute force attack or use a pre-computed identifier. Likely combinations of characters may be pre-computed if the number of bits used as well as the format of the identifier is known (e.g. 10 hexadecimal characters). [1] identifies a chart containing information from the MIT Auto-ID center that pinpoints the number of bits needed to uniquely identify items in a particular group.

5.2.3 Reader Threats

The use of malicious code may come as a surprise in an RFID system given the constraints placed on the technology (particularly the transponder). This is further intensified when considering the use of a passive read-only transponder. There is already a documented case in which a virus was maliciously loaded onto a tag for purposes of affecting the database [44]. In this case, simply presenting the tag to the reader may shut down an entire system by way of a malicious transponder. Although that case applied to an UHF tag, there is no implied limitation. A tag can be loaded with a destructive system command and set to operate at the frequency of the target reader [43].

Although the short read range of a transponder is a critical point in securing the front-end of the system, it may still be lengthened by the use of a directional high-gain antenna. Such antennas may be used to eavesdrop on communication between a tag and reader. After successfully recording the signal emitted by the reader, assuming a challenge-response algorithm is not used, the signal may be replayed via a clone. Such

activity may also occur without the use of a directional antenna. In this case, a rogue reader that may be hidden and used within close proximity of the target system can be used to aid in cloning as done by Jonathan Westhues [13].

Unless more than one reader is used for a particular application, physical damage to a reader could take out an entire system.

5.2.4 Database Threats

While the transponder and reader are major components of an RFID system, the database is just as critical. In most cases, while the tag holds a single identifying number, there has to be an entity that relates the key information specifically to that number. That is where the database comes in – linking the identifier to specific information. While this link is vital to the operation of an RFID system, it is also the weakest.

In the survey distributed as a part of this study, participants were asked how secure they feel databases are, resulting in 39.09% suggesting they feel databases are secure with a close 38.18% suggesting they feel databases are somewhat secure. This indicates that there is obviously a problem with the security of databases – and rightfully so!

Security of a Database (Rank)	%
Extremely Secure	1.82%
Very Secure	13.64%
Secure	39.09%
Somewhat Secure	38.18%
Not Secure	5.45%
No Response	1.82%

Table 3 – Survey of participants' thoughts on database security

According to [45], there have been approximately 495 documented cases of database breaches between January 10, 2005 and February 19, 2007, affecting in excess of 104,067,495 data records, including:

- February 15, 2005 breach of a ChoicePoint database in Alpharetta, GA, in which identity thieves created fraudulent accounts.

- December 25, 2005 breach of an Iowa State University database attributed to hacking that affected approximately 5,500 records comprised of credit card and social security numbers (SSN).

- March 14, 2006 breach of a General Motors database in Detroit, MI, in which an employee kept the SSNs of co-workers for the purpose of identity theft.

- May 3, 2006 breach of the U.S. Department of Veteran's Affairs in Washington, D.C. in which a laptop containing vital personal information such as SSNs and addresses of veterans discharged since 1975 was stolen from an employee's home, affecting approximately 28,600,000 records.

- February 2, 2007 breach of an U.S. Department of Veteran's Affairs, VA Medical Center database in Birmingham, AL in which an employee noted a missing or stolen hard drive, affecting 535,000 records.

- February 14, 2007 breach of an Iowa Department of Education database in which a hacker was able to view the files of 600 GED recipients.

Unfortunately, it does not appear as if the rate of database breaches is slowing down as there has been an increase from four documented breaches during the period of January 10 to February 19 in 2005 to 47 documented breaches in the same time period in

2007. [45] also provides an analysis of 2006 breaches, which attributes violations to outside hackers, insider malfeasance, human or software incompetence, non-laptop theft, and laptop theft.

This is important knowledge because a centralized mainstream RFID system would likely associate an identifying number to information relevant to financial records, medical records, classified or general access, or all of the above. [45] also provides in their analysis of 2006 database breaches, a breakdown of how each attributed violation affected a particular group: private sector, public sector, higher education, and medical centers. Based on the likely associations generated in a mainstream system, relevant groups would include the private sector, public sector, and medical centers. Of these, 40% of breaches in the private sector were associated with laptop theft, 44% in the public sector were associated with human/software incompetence, and 40% in medical centers were associated with laptop theft. So, simply put, while databases that are likely to be used in an RFID system may be advertised as being secure, they will still be vulnerable to the increasing number of threats currently affecting other database applications.

These threats loom further when considering how and if such databases are linked together. A 1989 amendment to the Privacy Act of 1974 (Section 9) states:

"Nothing in the amendments made by this Act shall be construed to authorize--

(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;

(2) the direct linking of computerized systems of records maintained by Federal agencies;

(3) the computer matching of records not otherwise authorized by law; or

(4) the disclosure of records for computer matching except to a Federal, State, or local agency." [46]

However, it does not particularly limit those in non-government sectors of data collection from linking records, except by existing laws. This means that unless prohibited by law, private organizations can link information between databases. Survey participants generally believe this is already being done as 80% of them responded that they believe databases are currently linked and 54.55% indicated they believe a large central database already exists!

Although 79% of participants disapprove of information about them being contained in one database being linked to other databases containing information about them, and 85.45% indicated they would be concerned if information on them from varying databases were consolidated into a large central database, it is likely that the introduction of a mainstream RFID system would do this. This concern is not limited only to survey participants. An August 16, 2005 testimony given by Pam Dixon, then Executive Director of World Privacy Forum, before the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality mentioned:

"Medical identity theft unfortunately may lead to the alteration of medical files… Digitization may in fact serve to exacerbate this problem, not solve it, particularly in the case of records that are networked." [47]

Given the information that has been presented, it is thereby concluded that a centralized mainstream RFID system will serve as a catalyst to linking databases (if not already done) that will result in an increased threat of compromising data due to the increased rate of database breaches that is currently observed. Until databases in general

receive better security protocols, they will continue to be a major weak link in RFID systems.

5.3 Current Countermeasures & Counter-countermeasures

5.3.1 Blocker Tags

The concept of blocking tags may also be used to secure a tag from rogue readers. However, the tag that has been proposed for purposes of security is more sophisticated than the method of blocking presented as a threat. In essence, the blocker tag functions under the auspices of DoS by jamming the reader; it exploits the tree-walking algorithm used by some readers for anti-collision purposes. It also inadvertently exploits the fact that in using this particular algorithm, readers can only read one tag at a time. (With the proper response from a tag, a reader can read the projected hundreds of tags per second.) When placed in the presence of a reader, the blocker tag effectively confuses the reader by sending out differing serial numbers, forcing it to walk every branch of the tree. An illustration of this algorithm may be found in Appendix B.

A problem with applying this technique to a tag implanted in a human is the fact that if the tag were implanted in a person, to be certain the tag is effective, a person may have to wear the blocker tag as if it were a band-aid or "hand-band" (although it may be possible for the person to wear it anywhere else on his or her person). If worn in either of these fashions, there is the possibility that it could either fall off or interfere with work and other activities. Additionally, consider the use of a blocker tag with such applications as credit cards and passports. While this may protect information in transit, once the card (or other transponder) is removed from the blocker tag to complete a transaction, it becomes vulnerable to attacks mentioned in section 5.3.

5.3.2 Cryptography

An obvious choice for securing data in an RFID system is the use of cryptography, either by way of encryption or some type of algorithm such as a challenge-response algorithm or public-key cryptography algorithm. While this is probably one of the best alternatives, implementation in RFID does have its flaws. In all cases, the physical size of a transponder will limit its memory and computing power. For now, this means that proven algorithms such as the RSA algorithm cannot be used. [43] mentions that current implementation of this option has been left to techniques incorporating relatively weak passwords. As an example, [43] cites the Mobil Speedpass utilizing a challenge-response algorithm that incorporated use of a 40-bit key. Although this carried on successfully for seven years before notice, this does raise concern given the nature of communication. This also causes several other concerns: the use of a method known as security-through-obscurity.

Security-through-obscurity is known as being a system's own worst enemy; preventing an outsider from having the opportunity to review the technique used could (and usually) result in the exploitation of undetected flaws. Despite this, many have taken to securing algorithms under terms of propriety rather than using an open protocol that has been tested rigorously.

5.3.3 Directional Antennas

The use of directional antennas for the tag and reader could aid in keeping data from straying too far away from the intended source and into unchartered territory. While this may be desirable as an additional aid for securing sensitive information, several factors would prevent it from being close to ideal. Tag orientation would play a

huge role in the acceptance rate of a system; this may be less suitable for daily applications as it is likely to cut down on the speed promised and desired by most systems. Ultimately, the tag would have to have a clear line-of-sight (LOS) with the reader for an acceptable read. LOS in an RFID system is typically less desirable since it may render the system comparable to some other systems it is proposed to replace.

5.3.4 Exploiting SNR

In this method, it is suggested that, "the signal-to-noise ratio of a reader query, as measured on an RFID tag, gives a rough indication of how close the tag is to the reader" [8]. A closer look at this concept reveals the strength of a signal varies as it propagates through the transmission medium while the noise typically remains constant; something that may be analyzed to determine the distance. So, in essence, if a tag were able to estimate the distance to the reader interrogating it, the tag could be programmed to not respond to a reader unless it is within a certain range [8].

The authors of [48] found that, "a minor variation on signal strength analysis does correlate tag distance to received energy." This roughly equates to the idea being extremely feasible. Although the equipment used in the experiments operated at 915 MHz, it may be possible to adapt such a technique for lower frequencies. However, there is only one problem: if this technique is used alone, a transponder will transmit data to a rogue reader placed within an acceptable range!

5.3.5 Kill Command

The kill command has been introduced primarily for use in transactions involving tagged merchandise. The way this technique works is that once scanned, a password can

be used to set the kill bit, which would prevent the tag from sending information if ever interrogated again. Unfortunately, as mentioned by [8], one drawback of the kill command is that once the tag has been "killed", there may be question as to whether or not it is still "alive", and if it really is killed, the process cannot be reversed. Even if it could be reversed, one should be concerned as to *who* can reverse it.

5.3.6 Physical Protection

As mentioned in Chapter 4, Section 1.1, a form of protecting passports incorporates the use of a Faraday cage housing. Of course this may be used with other forms of transponders and may be replaced by mu-metal or the alternative method of aluminum foil enveloping a thin layer of salt-water solution. While any of these may be used to enclose a transponder or line objects such as wallets, purses, and maybe one day clothing, the problem arises when the tag needs to be used. Removal from the source of protection would render the tag (and system) vulnerable for the duration of a transaction or as long as it is removed from the protective enclosure.

5.3.7 Soft Blocking

Soft blocking is a technique in which a program in the reader determines if it is okay to read a tag based on a privacy number received from the transponder. The problem with this technique is that a trust with the RFID reader needs to be established and cooperation from the reader is required [8]. Without trust and cooperation, the technique would be null and void. So, in the case of a rogue reader, this would not work, as the transponder has no way of protecting itself.

5.3.8 Tag Pseudonyms

The concept behind tag pseudonyms is that a transponder may hold a specified amount of ID numbers. Each time a person uses his or her transponder a new identification number is used. Problems with this approach include having to register all numbers in a tag with each location a person may choose to use his or her transponder. Also, if someone wanted to "take a person's identity," or steal products from a store, they would only need either one of the numbers (since they would all be registered) or they could continually interrogate the transponder until all numbers are found [8].

CHAPTER 6: An Innovative Method for Securing RFID Systems

One of the primary concerns of RFID systems is security. As discussed earlier, current security protocols for such systems are limited by the size and range of the transponder. For example, passive low-frequency transponders with a single identifying number that are constrained to a small size will not be able to hold a significant amount of memory, which in turn limits the complexity of any security protocol implemented. In addition, cost plays a major factor as the centralized mainstream implementation of RFID hinges on affordability – adding additional memory and functions without increasing the size of a transponder will effectively increase the cost and may, in some cases, eliminate the affordability factor or seriously compromise or dampen it.

Because mainstream RFID would incorporate applications that deal with medical and financial records and access control, it is imperative that security be designed at the forefront rather than introduced later. However, since that point has all but vanished, the next best thing is to look at how an RFID system can secure itself. A method of doing so surrounds the concept of fingerprinting an electronically produced signal.

6.1 RFID Fingerprinting

An on-going project at Iowa State University, the DILON project, presents a unique approach for fingerprinting electronically produced signals. This group believes that the components used in manufacturing electronic devices have minute variations because of imperfections in their construction [49]. Exploiting these variations can result in the characterization of a signal emitted from a device, thus resulting in a fingerprint for

the device. The group was quite successful in experiments performed using wired network cards; and, accordingly, the fingerprinting technique used for DILON has been identified as a technique that may be adapted for wireless communications and, ultimately, RFID systems.

In brief, the method described in [49] involves the observation and collection of signal data from several NICs produced by a single manufacturer and several NICs produced by alternative manufacturers, all operating under 10Mb Ethernet. Once the data is collected, a profile of the card is generated and a matched filter is used to distinguish between profiles. This methodology resulted in a favorable false reject rate (FRR), less than 1%, for devices from differing manufacturers.

In adopting this methodology for RFID, the matched filter may be used to distinguish between signals as done in the procedures for DILON. However, it may also be substituted with observing variations in the characteristic signal peaks found in the Fast Fourier Transform (FFT) of a signal. Due to time constraints, verification of this technique is left for future work. Instead, research is refocused to perform signal detection and characterization. Successful detection and characterization of a signal will lead to further confidence that the DILON technique may be applied to inductively coupled RFID systems.

6.1.1 Signal Detection and Characterization

For purposes of this study, signal detection involves successfully capturing and demodulating data transferred from the tag to the reader. Detection of data transmitted from the reader to the tag is not necessary since the premise of RFID fingerprinting is

distinguishing between transponders. Signal characterization involves successfully decoding the demodulated data to reveal the ID transmitted by a tag.

6.1.1.1 Signal Detection

The equipment used for signal detection included an oscilloscope, two inductors, an RFID reader, and two types of RFID tags. More specific information about the equipment is given in Table 4.

Equipment	**Information**
Inductance Coil	• 88 turns of 30 gauge magnet wire • Height: 3.49cm • Diameter: 17.78cm • Core: Cardboard
Oscilloscope	Tektronix Model DPO 4032 Digital Phosphor Oscilloscope
Reader	• RFID, Inc. Model 7000E-RO • Operating frequency: 125kHz

Tags	• RFID, Inc. Model 1775 Glass Ampoule Tag
	  • Read only
	  • Operating frequency: 125kHz
	  • ID: 10 hexadecimal characters
	  • Read time: 12ms to 50ms
	• RFID, Inc. Model 1778 Pill Tag
	  • Read only
	  • Operating frequency: 125kHz
	  • ID: 10 hexadecimal characters
	  • Read time: 12ms to 50ms

Table 4 - List of equipment and specifications used during study.

Since the system we are using is an inductively coupled system, a user (or intruder) will have to use inductance to detect communication between a tag and reader. Accordingly, the first experiment performed in this study is aimed at determining the maximum distance at which the powered reader can be detected. This is important from

a security standpoint because it gives an approximation of how far away someone (authorized or unauthorized) will need to be to detect a signal.

To determine the maximum distance at which the reader can be detected, one inductor is connected to the oscilloscope and the reader is powered. As shown in Figure 4, the observed maximum voltage level occurs when the reader is placed directly on top of the inductor (a distance of 0cm). From that point, the signal appears to fade exponentially.

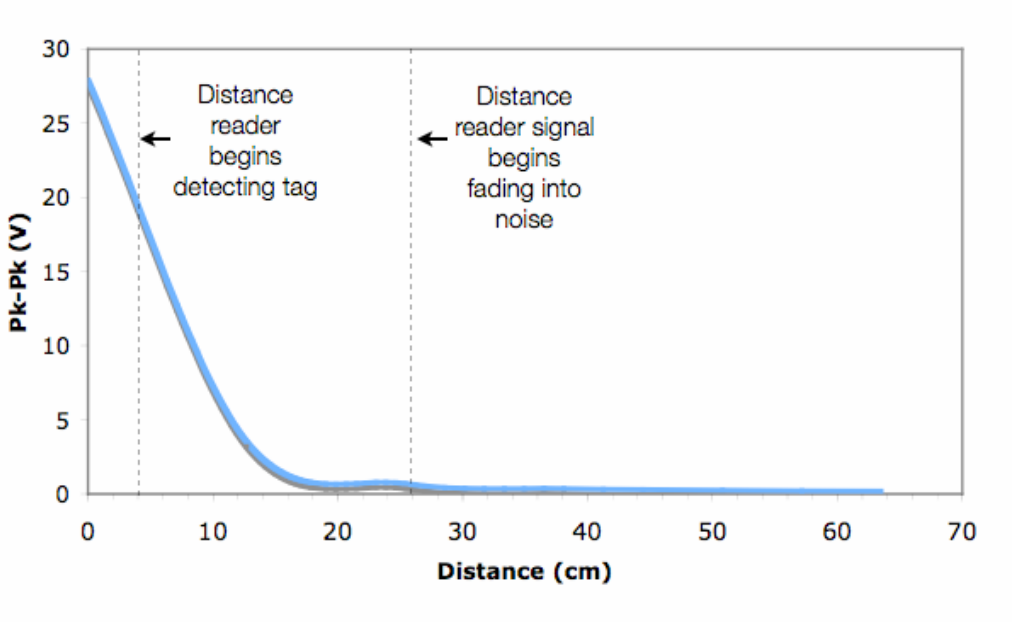


Figure 4 - Plot of observed voltage levels of a powered reader in relation to distance.

Next, the center frequency of the RFID system is verified. This must be done to ensure work from this point forward incorporates the correct center frequency. Again, one inductor is connected to the oscilloscope while the powered reader is placed atop the inductor. Given the equipment is advertised to operate at 125kHz, a sampling rate of 500kHz is selected and a record is taken. A Fast Fourier Transform (FFT) of the

collected data, as illustrated in Figure 5, shows that the center frequency of the reader is actually 128kHz. The same procedure is repeated with the two forms of tags selected for this study being separately placed atop the reader. This also yields a center frequency of 128kHz.

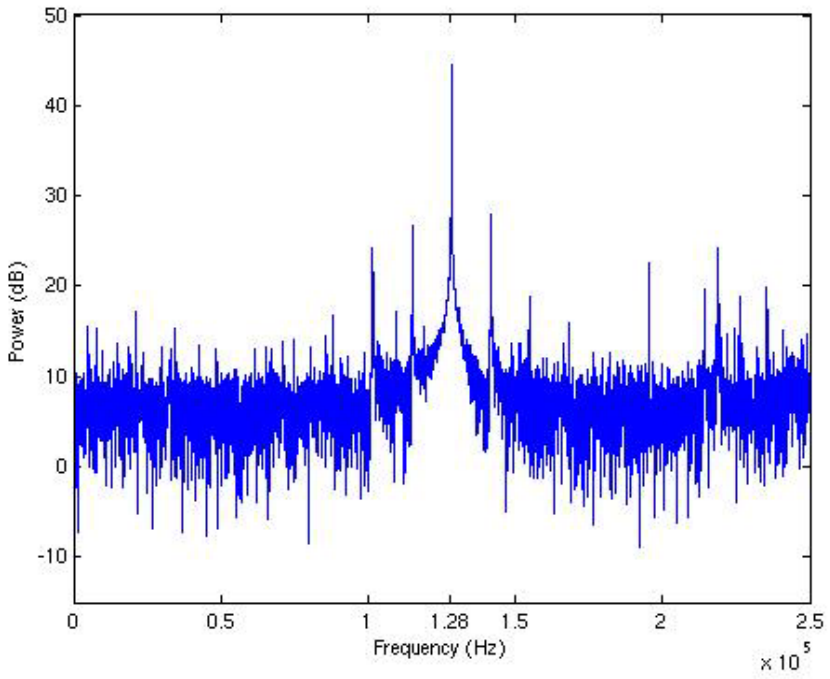


Figure 5 - Center frequency verification of reader.

In the final experiment, two inductors are attached to opposing ends of a cylinder with a height of 17.78cm and diameter of 16.83cm, creating a distance of 10.79cm between the inductors. The inductors are positioned such that, when facing each other, the coils appear to be wound in opposite directions. The two meeting ends of wire are tied together; and, when connected to the oscilloscope, are connected to the ground of the probe along with one of the free ends of coil. This setup is constructed to limit the amount of noise detected in the lab environment by a single coil. The reader is then placed atop the top inductor as shown in Figure 6.

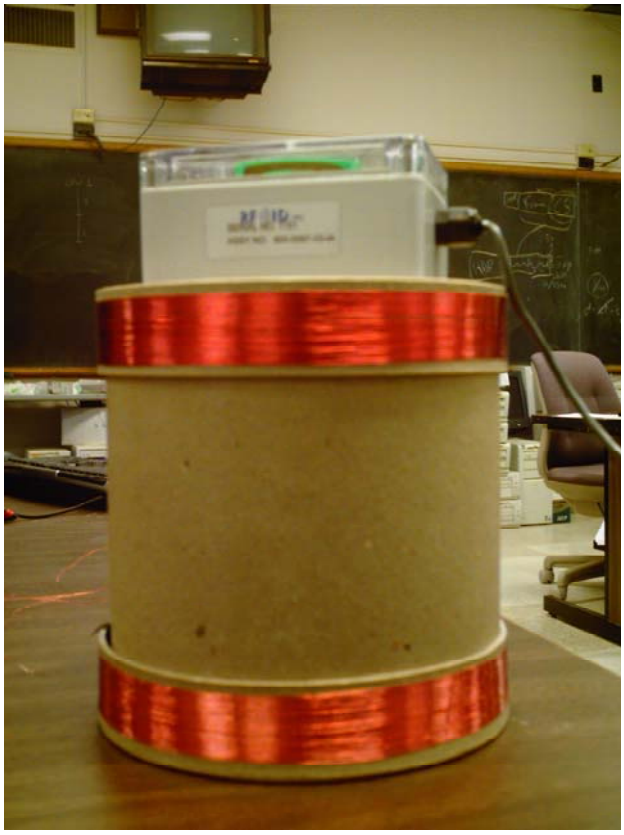


Figure 6 - Inductor setup with reader sitting on top coil.

Since finding the system actually operates at 128kHz, a new sampling rate of 2.5MHz is arbitrarily selected for oversampling, which provides a higher signal resolution than sampling at the Nyquist rate, $f_s = 2f_c$. When powered by the reader antenna, the tags continuously transmit data; so, data records are taken while a tag sits on top of the reader.

As shown in Table 4, the tag read time falls between 12ms and 50ms. To ensure a full data frame is recorded, records that are 400ms long are captured. A segment of a sample record is shown in Figure 7.

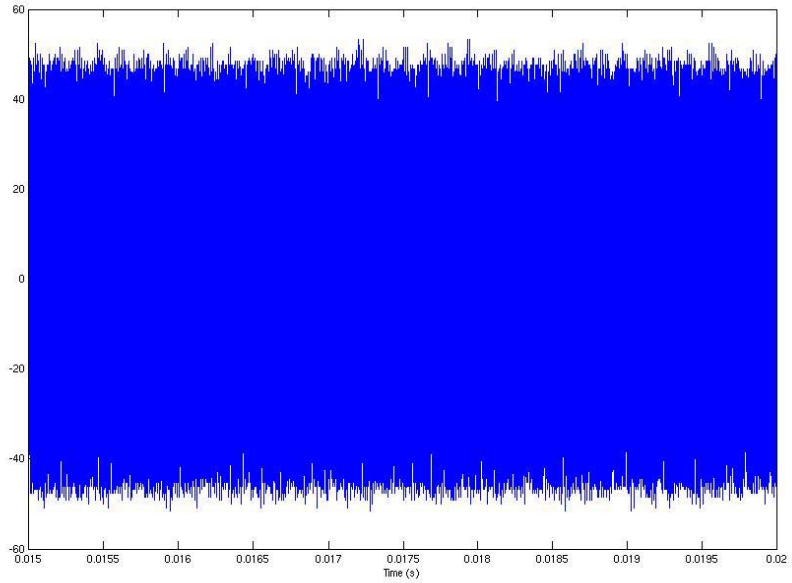


Figure 7 – 5ms segment of a 400ms data record.

To verify data has been captured, records are passed through an envelope detector, phase detector, and frequency detector – each of which is constructed in MATLAB. Given the nature of this system, AM modulation is expected; and, passing a record through an envelope detector should yield a demodulated signal. The phase detector and frequency detector are used to verify there is no phase or frequency modulation. The code used for constructing these detectors is given in Appendix C. Implementing this step indeed reveals data that is amplitude modulated with no phase or frequency modulation as demonstrated in Figure 8.

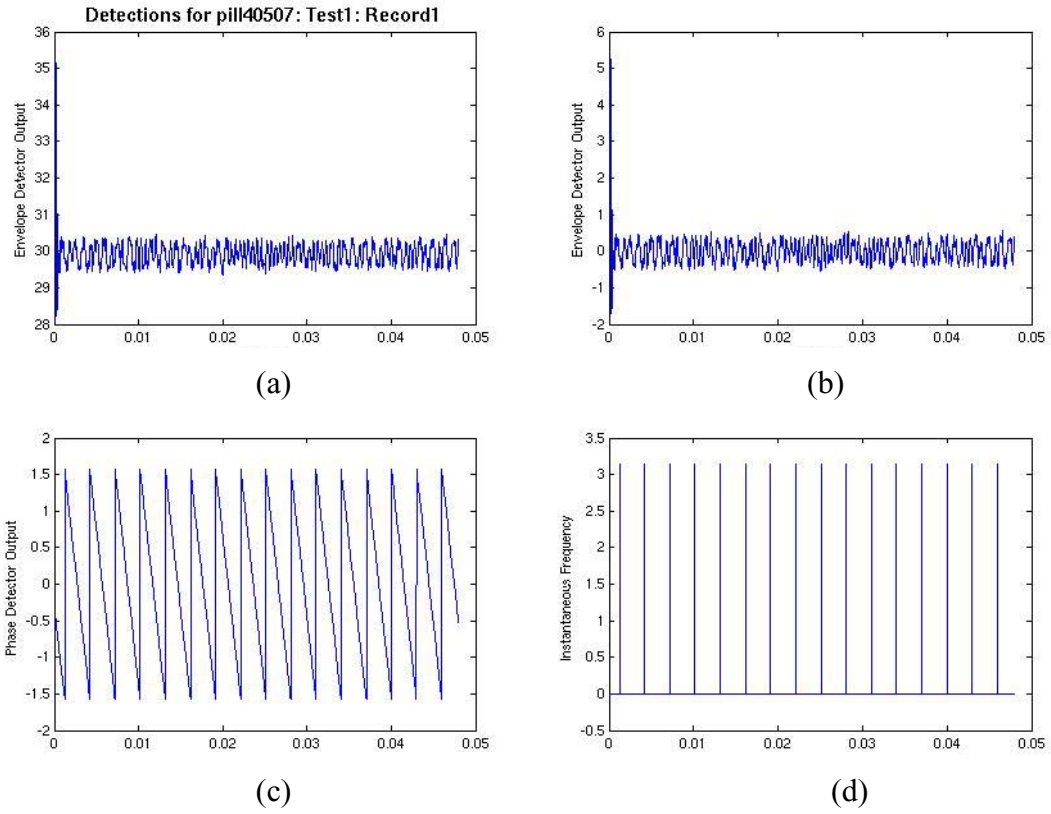
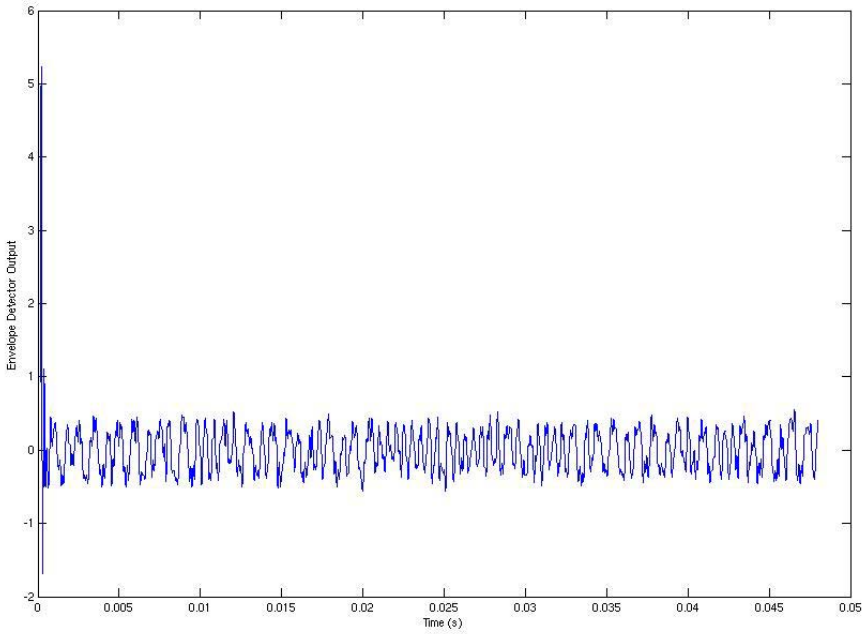


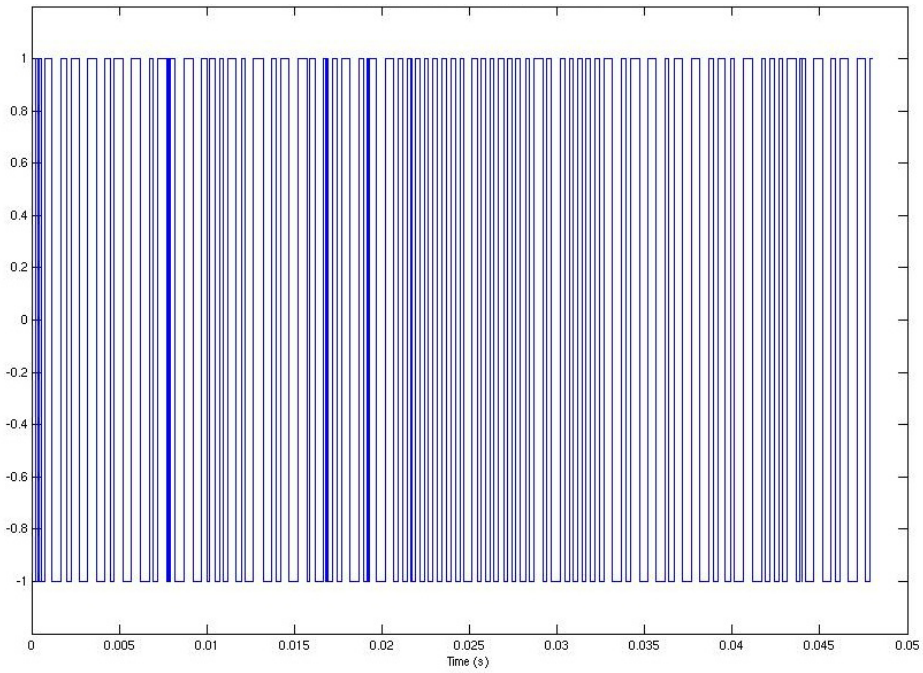
Figure 8 – 48ms clip of a 400ms record displaying output from (a) envelope detector, (b) average of envelope detector, (c) phase detector, and (d) instantaneous frequency detection.

6.1.1.2 Signal Characterization

Now that signal detection is complete, the arduous task of characterizing the signal begins. To help better understand the demodulated signal, the Signum function is applied to the data using the MATLAB sign() function. This produces the image shown in Figure 9b.



(a)



(b)

Figure 9 – (a) Plot of demodulated data before applying signum function. (b) Plot of demodulated data after applying the signum function.

As mentioned in the Introduction, there are a number of baseband coding techniques that may be used, including: NRZ, Manchester, Unipolar RZ, DBP, Miller, Differential, and PPC. Initially, several coding techniques are considered as candidates for the technique incorporated by our tags, among them Manchester Code and Differential Manchester Code. As suggested by [41], Manchester code is used for tag to reader communication in systems using load modulation with a sub-carrier. Reviewing the demodulated data also shows there is a noticeable similarity to Differential Manchester Code. Therefore, in order to decode the signal, the data is compared to both techniques.

In Manchester coding, a binary stream is coded by representing a '1' by a negative transition halfway into a bit period, and a '0' is represented by a positive transition halfway into a bit period. Observation of Figure 9b shows that the bit period is approximately 0.3ms, which lends to a read time of 24ms. For this example, the ID emitted from a pill tag is 0x010444A39C. Using Manchester coding, the expected sequence is that of Figure 10.

In Differential Manchester coding, a binary stream is coded by generating a symbolic '1' such that the first half of the bit period maintains the last half of the previous bit period; and, a '0' is generated such that the first half of the bit period is the inverse of the last half of the previous bit period. Figure 11 displays the expected waveform for the ID 0x010444A39C.

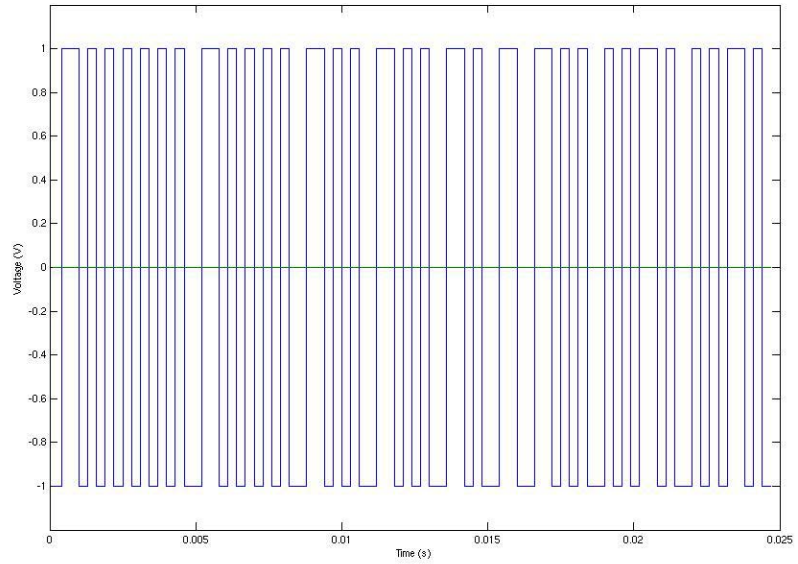


Figure 10 - Expected sequence when using Manchester encoding to encode 0x010444A39C. The first represented bit is '1', which is an assumed lock bit.

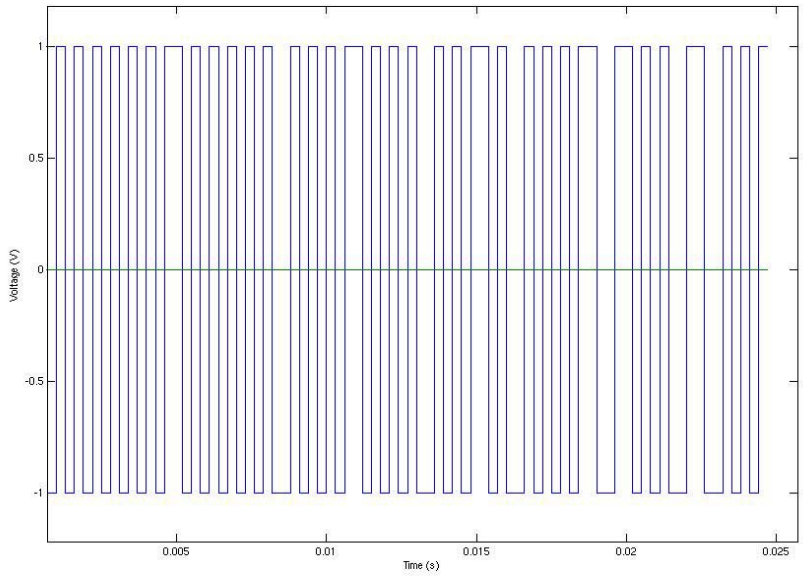


Figure 11 - Expected sequence when using Differential Manchester encoding to encode 0x010444A39C. The first represented bit is '1', which is an assumed lock bit.

In communications systems, it is expected that communication of information occurs in frames consisting of a start sequence followed by the data (in this case, the tag ID number) and a stop sequence. Manufacturer information reveals that a lock bit is included; so, it is assumed that this bit is also transmitted. Since additional information that would help reveal the frame sequence is not known, the data is visually checked for duplication, as well as used for hard bit detection. It is found that duplication occurs every 32ms. Therefore, it is expected that the read time for the system under testing is 32ms.

Three methods for hard bit detection are used in this phase of experimental work. The first method involves visually applying the rules for the aforementioned line coding techniques to decode the data and comparing the decoded bits to the expected bits. In addition to using the rules for those coding techniques with this method, the 32ms time period is utilized to estimate a bit period based on the communication of 41 bits. This produces a pattern in which a '1' could be represented as a positive or negative transition halfway into a bit period; and, a '0' could be represented as a single positive or negative pulse in a bit period. Unfortunately, use of this technique, referred to as *Special Case*, does not produce the expected bit pattern, even when inverted.

Another method used for hard bit detection involves recording the transitions from a 16ms segment of demodulated data, decoding those transitions, and comparing them with the expected bit sequence. Results from this technique may be seen in Table 5. While no exact match to the expected bit sequence is found, a dominant bit sequence is observed as the decoded sequence found after applying the rules for differential

Manchester, Pulse-Width Modulation (PWM), DBP, and Inverted Biphase Mark Code (BMC) appear to be identical.

Tag ID Number: 0x010444A39C

Expected Bit Sequence:
0000 0001 0000 0100 0100 0100 1010 0011 1001 1100

Observed Signal Transitions:
0010 1011 0010 1100 1101 0101 0101 0101 0100 1010 1010 1010 1011 0100 1010 101

Encoding Technique	Decoded Information
Biphase Mark Code (BMC)	0110 0100 0111 1111 1011 1111 1010 111x
Inverted BMC	1001 1011 1000 0000 0100 0000 0101 000x
DBP	1001 1011 1000 0000 0100 0000 0101 000x
Differential	1011 1110 1011 1010 1011 1111 1111 1111 1110 1111 1111 1111 1110 1110 1111 111x
Inverted Differential	0100 0001 0100 0101 0100 0000 0000 0000 0001 0000 0000 0000 0001 0001 0000 000x
Differential Manchester	1001 1011 1000 0000 0100 0000 0101 000x
Manchester	1110 1101 0000 0000 0111 1111 1001 111x
Inverted Manchester	0001 0010 1111 1111 1000 0000 0110 000x
Miller Code	Ruled out because of '10' states. This does not fit the behavior defined for this technique.
Modified Miller Code	Ruled out because of '00' states. This does not fit the behavior defined for this technique.
NRZ	0010 1011 0010 1100 1101 0101 0101 0101 0100 1010 1010 1010 1011 0100 1010 101x
PWM	1001 1011 1000 0000 0100 0000 0101 000x
Special Case	1011 1111 0011 0001 1000
Unipolar RZ	Ruled out because of '11' states. This does not fit the behavior defined for this technique.

Table 5 - Encoding techniques used to decode a 16ms segment of demodulated data with the observed transitions. The results from applying the rules for each technique are given in the column, Decoded Information.

The final method used for hard bit detection consists of: generating the expected bits for several line coding schemes in MATLAB based on an estimated bit period of

0.3ms (the width of the smallest significant pulse); printing the generated image as well as the image for the demodulated data; and, sliding the expected image across the data image to visually locate a match. This method rules out Manchester, Inverted Manchester, and NRZ as the line coding schemes used to encode the data. Although a complete match is not found using differential Manchester, portions of the images do match.

6.2 Future Work

Unfortunately, the methods used for hard bit detection did not produce an exact match to the expected bit sequence. However, there are several factors that may be taken into consideration. In implementing the methods discussed in Section 6.1.1.2, it was assumed that the most significant bit is communicated first and that no techniques such as bit stuffing or using a password to encrypt the ID before it is loaded onto the tag are used. Additional work may incorporate the assumption that the least significant bit is transmitted first and/or the other aforementioned techniques are used.

In the process of demodulating the signal, it was found that there is a low percentage of modulation. Despite this, there is still confidence that the DILON technique can be used for fingerprinting signals in inductively coupled RFID systems. Therefore, pending successful completion of signal characterization, much work will need to be done to achieve a tag fingerprint. As mentioned in Section 6.1, either the matched filter technique currently used for DILON will need to be incorporated, or the characteristic signal peaks found in the FFT of signals from various tags will need to be analyzed, to detect signal variation. If variation is observed then the concept of

fingerprinting an RFID device is deemed plausible and steps can be made to begin profiling tag signals.

There are pros and cons to moving forward with further exploration of this technique. As mentioned in the opening of this chapter, other countermeasures are faced with the obstacle of actually securing the tag rather than bestowing this responsibility exclusively on the reader. Unfortunately, RFID fingerprinting runs into this same problem as tag variability, and subsequent fingerprinting, would be determined by the reader. Where this technique differs from most is that no additional cost is forged onto transponders because of reliance on the tag's physical characteristics. Implementation may therefore be limited to a means by which to extract signal data from the reader and an additional "attachment" to the identifier in the system database. Moving forward with further exploration of this technique would therefore incorporate an analysis of the expected cost of implementation.

Other benefits this technique would celebrate include the expected ability to distinguish between a clone and the real tag – an advantage for the consumer in terms of the locations he or she may frequent. This means that a person may be less susceptible to having his or her identity *stolen and used* in a location he or she frequents. If the location happens to be an office satellite or national chain (e.g. stores and banks), it may even be possible for the fingerprint to become applicable at other locations. However, the downside of this technique is experienced when a successful clone is made and used at a

location or institution that the consumer has never visited. A profile could be successfully made and utilized without the original user's knowledge.

Another disadvantage is the fact that fingerprinting may be used to track an individual, or at least, pinpoint the locations he or she may have visited. While fingerprinting alone would not specify the time and date a person has been to a location, this does allow the ability to generalize a person's habits. This may also turn into an advantage since it could be used to fight or inhibit the ability of a clone being used to generate a profile without the original user's knowledge or consent. If a national network of "fingerprints" that keeps track of when and where new profiles are generated were to be established, it could be set to immediately alert an individual when a new profile is created and ask the person whose information is on file to authorize the new profile!

RFID fingerprinting should not be used alone. In fact, it should only serve to enhance the security of a system. For example, a credit card may be kept in a faraday cage housing or mu-metal lined wallet or pocketbook. Cryptographic measures should also be used to maintain data integrity, while RFID fingerprinting in conjunction with exploiting signal SNR may be used for verification.

CHAPTER 7: Conclusion

Radio frequency identification is a technology poised to become widely used in the future. Although there is a major reluctance to accept the technology among many people because of privacy and security issues, a group of advocates are forcefully pushing for further mainstream implementation. This has given rise to the question posed in the introduction of this thesis: how can successful use of this technology coexist with fears and concerns of privacy invasion and security risks?

The only way there can be coexistence is by gaining the confidence and trust of those people who are questioning the validity of the technology and showing them that it is secure and can maintain privacy [8]. One of the best ways to do this is to explore those problems that currently exist with the technology then propose ways to correct those problems. My hope is that by tackling the issue of security and social implications of radio frequency identification, problems that may occur with introducing this technology as a mainstream centralized system for identification are noticed and further action is taken to correct them.

RFID is still at a stage where it may not be too late to consider implementing strong security and privacy measures at the very critical design stage. This is most crucial when considering the concept of the, "Internet of Things." Modern day computer networks have numerous complications, some (not all) of which have been given in Chapter 5 as problems RFID is beginning to face – problems that were not perceived as threats with its introduction. Building a concept based off of an already ailing system

will only result in future unwanted complications. While countermeasures have been given that could help bypass those issues that RFID has encountered, it has been shown that those countermeasures can become the seed for counter-countermeasures, a process that will eventually result in an RFID warfare cycle. While this cycle is inevitable, considering additional creative ways of securing a system will only help to strengthen the current level of security. That is why RFID fingerprinting is proposed.

The concept of RFID fingerprinting has been introduced as a technique for enhancing current security measures. It relies on the physical characteristics of the transponder and the management of a signal profile created in relation to signals transmitted by the tag and received by the reader. While the concept theoretically sounds feasible, experiments were performed to determine feasibility as related to signal detection and characterization.

It has been shown that the signal resulting from communication between a passive tag and a reader can be successfully detected. However, signal characterization is currently inconclusive. In attempting to decode demodulated data, several possible factors were not considered, including: communication of the least significant bit first, bit stuffing, and data encryption. Despite this, there is still confidence that the detected signals can be successfully characterized and confidence that the fingerprinting technique provided by DILON can be applied to inductively coupled RFID systems.

REFERENCES

[1] K. Albrecht and L. McIntyre, Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID, Tennessee: Nelson Current, 2005.

[2] "The History of RFID Technology," RFID Journal [Online periodical] Available: http://www.rfidjournal.com/article/articleprint/1338/-1/129/ [Accessed December 18, 2006].

[3] "The Theremin Page", The Musical Museum, London, England [Online document] Available: http://www.musicalmuseum.co.uk/theremin.html [Accessed December 18, 2006].

[4] M. Cardullo and W. Parks, III, "Transponder Apparatus & System," U.S. Patent 3,713,148, January 23, 1973.

[5] G. Works, J. Murray, E. Ostroff, N. Freedman, "Remotely Powered Transponder," U.S. Patent 3,745,569, July 10, 1973.

[6] J. Landt, "The History of RFID," Potentials, IEEE, vol. 24, no. 4, pp.8-11, Oct.-Nov. 2005.

[7] K. Finkenzeller, RFID Handbook: Radio-Frequency Identification Fundamentals and Applications, New York: Wiley & Sons Ltd, 1999.

[8] S. Garfinkel and B. Rosenberg, RFID: Applications, Security, and Privacy, New Jersey: Pearson Education, 2006.

[9] S. Sarma, S. Weis, D. Engels. "RFID Systems and Security and Privacy Implications", [Online document] Available: http://theory.lcs.mit.edu/~sweis/pdfs/ches-rfid.pdf [Accessed January 15, 2006].

[10] S. Lahiri, RFID Sourcebook, New Jersey: IBM Press, 2006.

[11] "RFID". [Online document] Available: http://en.wikipedia.org/wiki/RFID#Current_usage [Accessed January 15, 2006].

[12] "RFID 101: RFID system frequency ranges." [Online periodical] Available: http://www.rfid-101.com/rfid-frequencies.htm [Accessed March 16, 2006].

[13] J. Westhues, "Demo: Cloning a Verichip", January 2006. [Online] Available: http://cq.cx/verichip.pl [Accessed April 20, 2006].

[14] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues, "The Security Implications of VeriChip Cloning", [Online document] Available: http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/verichip/Verichip.pdf [Accessed January 21, 2007].

[15] C. Perakslis and R. Wolk, "Social Acceptance of RFID as a Biometric Security Method" Proceedings of the International Symposium on Technology and Society (ISTAS 05), June 2005, pp. 79-87.

[16] Auto-ID Labs at MIT. [Online] Available: http://autoid.mit.edu/CS/ [Accessed November 1, 2006].

[17] "Michielson Watch: DEFCON Hackers", RFID News, Aug. 2, 2005. [Online] Available: http://www.rfidnews.org/weblog/2005/08/02/michielsen-watch-defcon-hackers/ [Accessed February 3, 2007].

[18] United States. Data Privacy & Integrity Advisory Committee. The Use of RFID for Human Identity Verification, Rep. 2006-02. Department of Homeland Security, 2006.

[19] "The Technology Adoption Life-cycle," [Online] Available: http://ist-socrates.berkeley.edu/~fmb/articles/lifecycle/ [Accessed April 12, 2007].

[20] T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. O'Hare, "RFID Payment Card Vulnerabilities Technical Report", RFID Consortium for Security and Privacy (CUSP), Technical Report, October 2006.

[21] A. Marcella and C. Stucki, Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues, Hoboken, N.J.: John Wiley & Sons, Inc., 2003.

[22] A. Juels, D. Molnar, and D.Wagner, "Security & Privacy Issues in E-passports", Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM 05), Sept. 2005.

[23] United States. Electronic Passport, Code of Federal Regulations (CFR) 22 Part 51, Department of State, 2005. [Online] Available: http://edocket.access.gpo.gov/2005/05-21284.htm [Accessed February 3, 2007].

[24] W. Dizard, III, "E-Passport's first deployment", Government Computer News, Oct. 9, 2006. [Online] Available: http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn&story.id=42249 [Accessed February 3, 2007].

[25] W. Rash, "European Union Will Not Regulate RFID – For Now", EWeek, March 15, 2007. [Online periodical] Available: http://www.eweek.com/article2/0,1895,2104417,00.asp?kc=EWNAVEMNL031607EOAD [Accessed March 16, 2007].

[26] A. Graafstra, "Hands On: How Radio-Frequency Identification and I got personal," IEEE Spectrum, vol. 44, no. 3, pp. 18-23, March 2007.

[27] "VeriMed Patient Identification" [Online informational] Available: http://www.verimedinfo.com [Accessed April 20, 2006].

[28] CASPIAN, "FDA Letter Raises Questions about VeriChip Safety, Data Security", October 2004. [Online] Available: http://www.spychips.com/devices/verichip-fda-report.html [Accessed March 20, 2006].

[29] D. Tillman, FDA Letter to James Santelli of Digital Angel Corporation, October 2004. [Online document] Available: http://www.spychips.com/devices/verichip-fda-letter.pdf [Accessed March 20, 2006].

[30] "Revelations 13:16-18", The Holy Bible, New International Version, Grand Rapids, M.I.: The Zondervan Corporation, 2001.

[31] B.A. Robinson, "Religions of the World: Numbers of adherents; names of houses of worship; names of leaders; rates of growth…", Ontario Consultants on Religious Tolerance, March 24, 2006. [Online] Available: http://www.religioustolerance.org/worldrel.htm [Accessed March 11, 2007].

[32] "Real ID Act of 2005 Driver's License Title Summary", National Conference of State Legislatures. [Online] Available: http://www.ncsl.org/standcomm/sctran/realidsummary05.htm [Accessed April 2, 2007].

[33] N. Gaouette, "Real ID Act postponed two years", Los Angeles Times, March 22, 2007. [Online periodical] Available: http://www.latimes.com/news/printedition/asection/la-na-realid2mar02,1,5780163.story?coll=la-news-a_section%3A&ctrack=1&cset=true [Accessed March 11, 2007].

[34] "Children & RFID Systems: Brittan School's RFID-tagging of children", Electronic Privacy Information Center, June 9, 2005. [Online] Available: http://www.epic.org/privacy/rfid/children.html [Accessed April 18, 2006].

[35] M.C. O'Connor, "RFID Takes Attendance—and Heat", RFID Journal, February 16, 2005. [Online periodical] Available: http://www.rfidjournal.com/article/articleview/1408/1/1/ [Accessed April 18, 2006].

[36] K. Foster and J. Jaeger, "RFID Inside: The murkey ethics of implanted chips," IEEE Spectrum, vol. 44, no. 3, pp. 24-29, March 2007.

[37] H. Wolinsky, "P&G, Wal-Mart store did secret test of RFID", Chicago Sun-Times, November 9, 2003. [Online periodical] Available: http://www.findarticles.com/p/articles/mi_qn4155/is_20031109/ai_n12525588 [Accessed March 11, 2007].

[38] A. Newitz, " The RFID Hacking Underground," Wired, no. 14.05, n.d. [Online] Available: http://www.wired.com/wired/archive/14.05/rfid_pr.html [Accessed January 22, 2007].

[39] "Hitachi Unveils RFID Tag Smaller Than Speck of Dust", Fox News, February 26, 2007. [Online periodical] Available: http://www.foxnews.com/story/0,2933,254686,00.html [Accessed February 26, 2007].

[40] T. Scharfield, "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design," M.S. Thesis, Massachusetts Institute of Technology, Cambridge, MA, 2001.

[41] K. Finkenzeller, RFID Handbook, 2nd ed., R. Waddington, Trans., Chichester, West Sussex, England: John Wiley & Sons Ltd., 2003.

[42] "RFID White Paper", July 2004. [Online document] Available: http://www.rmsomega.com/documents/RFID_White_Paper_ScanSource_000.pdf [Accessed April 27, 2006].

[43] F. Thornton, B. Haines, A. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt, RFID Security, Rockland, M.A.: Syngress Publishing, Inc., 2006.

[44] J. Best, "RFID viruses? Don't panic", Silicon.com, March 16, 2006 [Online periodical] Available: http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39157280,00.htm [Accessed April 18, 2006].

[45] "A Chronology of Data Breaches", Privacy Rights Clearinghouse, February 19, 2007. [Online] Available: http://www.privacyrights.org/ar/ChronDataBreaches.htm [Accessed February 19, 2007].

[46] United States. “The Privacy Act of 1974”, 5 U.S.C. §552a. Department of Justice, 2003. [Online] Available: http://www.usdoj.gov/oip/privstat.htm [Accessed November 1, 2006].

[47] “Testimony of Pam Dixon, Executive Director World Privacy Forum Before the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality”, World Privacy Forum, August 16, 2005. [Online document] Available: http://www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html [Accessed February 19, 2007].

[48] K. Fishkin, S. Roy, and B. Jiang, “Some Methods for Privacy in RFID” [Online document] Available: http://www.intel-research.net/Publications/Seattle/062420041517_243.pdf [Accessed April 22, 2006].

[49] R. Gerdes, T. E. Daniels, M. Mina, and S. Russell, “Device identification via analog signal fingerprinting: A matched filter approach,” Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS 06), San Diego, California, Feb. 2006.

BIBLIOGRAPHY

[1] "Gone in 20 Minutes: using laptops to steal cars", Leftlane News, May 3, 2006. [Online periodical] Available: http://www.leftlanenews.com/2006/05/03/gone-in-20-minutes-using-laptops-to-steal-cars/ [Accessed January 21, 2007].

[2] "Hackers can crack car-key codes", Consumer Reports.org, Dec. 2005. [Online periodical] Available: http://www.consumerreports.org:80/cro/cars/hacking-car-security-1205-keyless-entry-system-car-security-system/index.htm [Accessed January 21, 2007].

[3] "Innovation Adoption Curve (Rogers)," 12Manage, April 9, 2007. [Online] Available: http://www.12manage.com/methods_rogers_innovation_adoption_curve.html [Accessed April 7, 2007].

[4] "Shrouds of Time: The history of RFID," AIM, ver. 1, Oct. 2001.

[5] CASPIAN. "Verichip RFID Implant Hacked!", January 2006. [Online periodical] Available: http://www.spychips.com/press-releases/verichip-hacked.html [Accessed April 20, 2006].

[6] T. Espiner, "RFID 'not safe from DoS attacks'", Silicon.com, April 18, 2006. [Online periodical] Available: http://software.silicon.com/security/0,39024655,39158120,00.htm [Accessed April 18, 2006].

[7] Federal Communications Commission, "Part 15 – Radio Frequency Devices," 2005 CFR Title 47, 2005. [Online document] Available: http://www.access.gpo.gov/nara/cfr/waisidx_05/47cfr15_05.html [Accessed January 15, 2006].

[8] K. Fishkin and S. Roy, "Enhancing RFID Privacy via Antenna Energy Analysis" presented at MIT RFID Privacy Workshop, Boston, MA 2003.

[9] S. Garfinkel, Database Nation: The Death of Privacy in the 21st Century, Sebastopol, CA: O'Reilly & Associates, Inc., 2000.

[10] B. Glover and H. Bhatt, RFID Essentials, Sebastopol, CA: O'Reilly Media, Inc., 2006.

[11] Impinj, "The RFID Tag Antenna: Orientation Sensitivity," Impinj, 2005. [Online document] Available: http://www.impinj.com/files/MR_00_TB_00020_AntennaDiversity.pdf [Accessed April 22, 2006].

[12] H. Lee and J. Kim, “Privacy threats and issues in mobile RFID”, Proceedings of the First International Conference on Availability, Reliability and Security (ARES 06), April 2006.

[13] N. Lomas, “How Orwellian can you get?”, Silicon.com, Oct. 17, 2006. [Online periodical] Available: http://networks.silicon.com/lans/0,39024867,39163311,00.htm [Accessed January 22, 2007].

[14] E. Nakashima, “Enjoying Technology’s Conveniences But Not Escaping Its Watchful Eyes”, Washington Post, Jan. 16, 2007. [Online periodical] Available: http://www.washingtonpost.com/wp-dyn/content/article/2007/01/15/AR2007011501304_pf.html [Accessed January 19, 2007].

[15] T. Phillips, T. Karygiannis, and R. Kuhn, “Security Standards for the RFID Market”, Security & Privacy Magazine, IEEE, vol. 3, no. 6, pp. 85-89, Nov.-Dec. 2005.

[16] M. Rieback, B. Crispo, A. Tanenbaum, “Is Your Cat Infected with a Computer Virus?” PERCOM 06, pp. 169-179, Fourth IEEE International Conference on Pervasive Computing and Communications, 2006.

[17] J. Schwartz, “Researchers See Privacy Pitfalls in No-Swipe Credit Cards”, The New York Times, Oct. 23, 2006. [Online periodical] Available: http://www.nytimes.com/2006/10/23/business/23card.html?ex=1319256000&en=76401b1601fc06e3&ei=5090 [Accessed January 21, 2007].

[18] S. Shepard, RFID: Radio Frequency Identification, New York, N.Y.: McGraw-Hill, 2005.

[19] R. Singel, “Feds Leapfrog RFID Privacy Study”, Wired News, Oct. 30, 2006. [Online periodical] Available: http://www.wired.com/news/technology/1,72019-0.html [Accessed January 22, 2007].

APPENDIX A: Acronyms

Chapter 1

RFID	Radio Frequency Identification
ASK	Amplitude Shift Keying
DBP	Differential Biphase
EAS	Electronic Article Surveillance
EEPROM	Electrically Erasable Programmable Read-Only Memory
EM	Electromagnetic
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FRAM	Ferromagnetic Random Access Memory
FSK	Frequency Shift Keying
HF	High Frequency
IRE	Institute of Radio Engineers
IFF	Identification Friend or Foe
ISM	Industrial, Scientific, Medical
LF	Low Frequency
NRZ	Non-Return to Zero
PPC	Pulse-Pause Code
PSK	Phase Shift Keying
RADAR	Radio Detection and Ranging
SRAM	Static Random Access Memory
UHF	Ultra-High Frequency

Chapter 2

CASPIAN	Consumers Against Supermarket Privacy Invasion and Numbering
DILON	Detecting Intrusion at Layer One
NIC	Network Interface Card

Chapter 3

ACL	Access Control List
EAS	Electronic Article Surveillance

Chapter 4

DHS	Department of Homeland Security (United States)
FDA	Food and Drug Administration (United States)
ICAO	International Civil Aviation Organization
PDA	Personal Digital Assistant

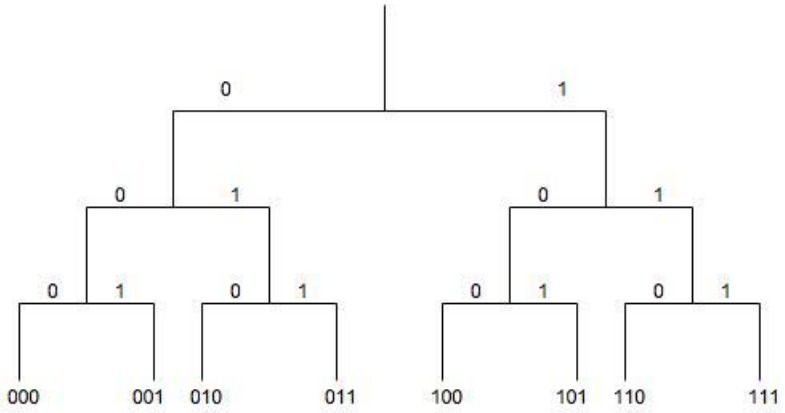
Chapter 5

DoS	Denial-of-Service
EPC	Electronic Product Code
ISO	International Organization for Standardization
NCVHS	National Committee on Vital Health Statistics
SSN	Social Security Number

Chapter 6

FFT	Fast Fourier Transform

APPENDIX B: Illustration of a Tree-Walking Algorithm



Above is a visual example of the tree-walking algorithm used by some readers. When a reader responds with its number, the number is sent through a tree such as the one above, significant bit first. The tree is traversed until the tag's number is found in one of the branches. In the case of the example above, the serial numbers are shown at the bottom as 000 – 111.

On a normal basis, the tree is quickly traversed as one side can be completely eliminated based on the first bit alone. However, when a blocker tag is introduced, multiple numbers are sent at the same time, confusing the reader as to which side to take first. So, the entire tree is traversed in an effort to find the transmitted numbers, which may take a considerable amount of time to accomplish.

APPENDIX C: Supporting MATLAB Code

This appendix contains code we created in MATLAB to aid in the signal detection and characterization process.

---

1. Signal Analysis Function

```
function [] = sig_analysis(data, descriptor, testday, testnum, recordnum, fs, fc, n, W, M)

%
% Purpose: This function serves as the main function for
% analyzing the RFID signals.  It calls two functions – sig_fft() and
% signal_detectors().
%
% Variables:
% data – data vector being analyzed
% descriptor - type of transponder used in data collection
% testday - day test took place
% testnum - number of the test taken on testday
% recordnum - a record number from testnum
% fs - sample frequency
% fc - center frequency
% n - filter order for Chebyshev Type II filter
% Rs - for Chebyshev filter
% W - for Chebyshev filter
% M - filter order for Moving Average filter
%
% Output: There is no output for this function.  It only produces
% figures generated by called functions
%

% Obtain the FFT of the signal (this also shows a plot of the data)
  sig_fft(data, fs);

% Perform Envelope and Phase Detection
  [mod_envelope, modified_phase, modified_freq]
          = signal_detectors(data, descriptor, testday, testnum, samplenum, fs, fc, n, W);
```

2. Signal Time Series Plot and FFT

```
function [] = sig_fft(data, sampling_rate)

%
% Purpose:  The purpose of this function is to plot the raw data
% and obtain an FFT of the data.
%
% Variables:
% data, the data vector being analyzed
% sampling_rate, the sampling rate used to obtain the raw data
%
% Output:  There is no output for this function.  It produces
% figures for analysis.
%

% Generate the time vector
k = length(data)/sampling_rate;

t = 0:length(data)-k;

t = t./sampling_rate;

% Plot the time series data
figure; plot(t, data);
xlabel('Time (s)');

% Obtain the FFT of the data
n = length(data);

f = (0:n-1)*sampling_rate/n;

fftsignal = fft(data);

% Plot the FFT in dB
figure; plot(f, 10*log10(abs(fftsignal)));
xlabel('Frequency (Hz)'); ylabel('Power (dB)');
```

3. Signal Detector Function

```
function [mod_envelope, modified_phase, modified_freq]
            = signal_detectors(data, descriptor, testday, testnum, samplenum, fs, fc, n, W)


%
% Purpose:  The purpose of this function is to provide envelope,
% phase, and frequency detection by implementing an envelope
% detector.  Output from the envelope detector is used for
% phase and frequency detection.
%
% Input Variables:
% filename, name of file containing data
% fs, sampling rate (Hz)
% n, filter order
% Rs, stopband ripple (dB)
% W, cutoff frequency for filter
%
% Output:
% mod_envelope, modified envelope detector output
%

% Build a Butterworth filter
Wn = W/(fs/2);              % Normalized frequency
[b, a] = butter(n, Wn,'low');

% Envelope Detection
y = abs(data);

% Filter the absolute value of the data
envelope = filter(b, a, y);


% Phase Detection
t = 0:1/fs:(1/fs)*length(data); % Time vector

% Verify the time and data vectors are the same length
if (length(t) > length(data))
   v = length(t) - length(data);
   t = 0:1/fs:(1/fs)*length(data)-v*(1/fs);
end

% The Envelope Detector
sig1 = sin(2*pi*fc*t);
sig2 = cos(2*pi*fc*t);

track1 = sig1'.*data;
track2 = sig2'.*data;
```

```
% Filter the absolute value of the data
filter_output1 = filter(b, a, track1);
filter_output2 = filter(b, a, track2);

output = filter_output1./filter_output2;

% Phase Detection
phase = atan(output);


% Frequency Detection
freq = diff(phase);

% The first 430 points are artifacts of the filter, so remove them.
for i = 431:length(envelope)
   modified_envelope(i-430, 1) = envelope(i);
end

for i = 431:length(phase)
   modified_phase(i-430, 1) = phase(i);
end

for i = 431:length(freq)
   modified_freq(i-430, 1) = freq(i);
end


% Average the output of the envelope detector.
envelope_avg = mean(modified_envelope);
mod_envelope = modified_envelope - envelope_avg;

t2 = 431/fs:1/fs:(1/fs)*length(data); % A new time vector

p = length(mod_envelope);

f = (0:p-1)*fs/p;                    % Frequency

% Plot the output from the detectors.
figure;
subplot(2, 2, 1); plot(t2, modified_envelope); xlabel('Time (s)'); ylabel('Envelope Detector
Output');
title(['Detections for ', descriptor, int2str(testday), ': Test', int2str(testnum), ': Record',
int2str(samplenum)], 'fontsize', 14, 'fontweight', 'bold');
subplot(2, 2, 2); plot(t2, mod_envelope); xlabel('Time (s)'); ylabel('Envelope Detector Output');
subplot(2, 2, 3); plot(t2, modified_phase); xlabel('Time (s)'); ylabel('Phase Detector Output');
subplot(2, 2, 4); plot(modified_freq); xlabel('Datapoints'); ylabel('Instantaneous Frequency');

figure;
plot(t2, mod_envelope); xlabel('Time (s)'); ylabel('Envelope Detector Output'); title('Averaged
Envelope Detector Output');
```

```
figure;
plot(f, 10*log10(abs(mod_env_fft))); xlabel('Frequency (Hz)'); ylabel('Power'); title('FFT of
Averaged Envelope Detector Output');
```